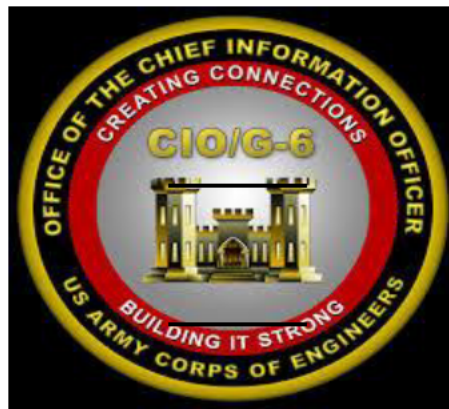


# **TASK ORDER (TO)**

**47QFCA21F0001  
Modification P00024  
December 22, 2022**

## **Revolutionary Information Technology Services (RITS)**

**in support of the:**



## **United States Army Corps of Engineers (USACE) Office of the Chief Information Officer (OCIO/G-6)**

**Issued to:**

**Science Applications International Corporation (SAIC)  
(GSA) Alliant 2 Unrestricted Governmentwide Acquisition Contract (GWAC), Multiple  
Award, Indefinite Quantity (IDIQ) Contract**

**Issued by:**

**The Federal Systems Integration and Management Center (FEDSIM)  
1800 F Street, NW (QF0B)  
Washington, D.C. 20405**

**November 30, 2020**

**FEDSIM Project Number 47QFCA21Z1082**

**TO 47QFCA21F0001  
P00024**

## SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

### B.1 GENERAL

The work shall be performed in accordance with all Sections of this Task Order (TO) and the contractor's Basic Contract, under which the resulting TO will be placed.

### B.2 CONTRACT ACCESS FEE (CAF)

The General Services Administration's (GSA) operating costs associated with the management and administration of this Contract are recovered through a CAF. In accordance with the Alliant base contract, the CAF shall be 0.75 percent of the total TO value with a cap of \$100,000 per year per order (when order is in excess of \$13.3M per order year). This TO shall have a separate Contract Line Item Number (CLIN) to cover this access fee, and this CAF shall be obligated at TO Award (TOA).

### B.3 ORDER TYPES

The contractor shall perform the effort required by this TO on a Cost-Plus-Award-Fee (CPAF) basis for:

- a. Mandatory Labor CLINs 0001, 1001, 2001, 3001, and 4001
- b. Optional Labor CLINs 0002, 1002, 2002, 3002, and 4002

The contractor shall perform the effort required by this TO on a Not-to-Exceed (NTE) Cost Reimbursement (CR) basis for:

- a. Long-Distance Travel CLINs 0003, 1003, 2003, 3003, and 4003
- b. CAF CLINs 0006, 1006, 2006, 3006, and 4006

The contractor shall perform the effort required by this TO on a Not-to-Exceed (NTE) Plus-Fixed-Fee (CPFF) basis for

- a. Tools CLINs 0004, 1004, 2004, 3004, and 4004
- b. Other Direct Costs (ODCs) CLINs 0005, 1005, 2005, 3005, and 4005

The Accounting for Army Manpower Reporting CLINs 0007, 1007, 2007, 3007, and 4007 are Not Separately Priced (NSP).

### B.4 SERVICES AND PRICES/COSTS

Long-distance travel is defined as travel over 75 miles from an employee's permanent duty Fstation. Local travel will not be reimbursed.

The following abbreviations are used in this price schedule:

CAF	Contract Access Fee
CLIN	Contract Line Item Number

## SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

CPAF	Cost-Plus-Award-Fee
NSP	Not Separately Priced
NTE	Not-to-Exceed
ODC	Other Direct Cost
QTY	Quantity

## SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

### B.4.1 BASE PERIOD:

#### MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
0001	Labor (Tasks 1–6)	(b) (4)		\$ 141,168,058

#### OPTIONAL CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
0002	Labor (Task 7)	(b) (4)		\$2,965,950.00

#### COST-REIMBURSEMENT TRAVEL CLIN

CLIN	Description		Total NTE Price
0003	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	\$5,000,000

#### CPFF TOOLS, and ODC CLINs

CLIN	Description	Cost	Fixed Fee	Total NTE Price
0004	Tools Including Indirect Handling Rate (b) (4) and (b) (4) fixed fee	(b) (4)	(4)	\$43,405,000
0005	ODCs Including Indirect Handling Rate (b) (4) and (b) (4) Fee			\$38,000,000

#### CAF

CLIN	Description		Total Ceiling Price
0006	CAF	NTE	\$100,000

#### ACCOUNTING FOR CONTRACTOR MANPOWER REPORTING

CLIN	Description		Total Price
0007	Accounting for Contractor Manpower Reporting		NSP

**TOTAL CEILING BASE PERIOD CLINs:**

**\$230,639,008.00**

### B.4.2 FIRST OPTION PERIOD

#### MANDATORY CPAF LABOR CLIN

TO 47QFCA21F0001  
P00024

PAGE B-4

## SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

CLIN	Description	Cost	Award Fee	Total CPAF
1001	Labor (Tasks 1–6)	(b) (4)	(b) (4)	\$154,506,592.00

### OPTIONAL CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
1002	Labor (Task 7)	(b) (4)		\$6,049,844.00

### COST-REIMBURSEMENT TRAVEL CLIN

CLIN	Description		Total NTE Price
1003	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	\$5,000,000

### CPFF TOOLS, and ODC CLINs

CLIN	Description	Cost	Fixed Fee	Total NTE Price
1004	Tools Including Indirect Handling Rate (b) (4) and (b) (4) fixed fee	(b) (4)	(4)	\$52,000,000
1005	ODCs Including Indirect Handling Rate (b) (4) and (b) (4) Fee			\$65,000,000

### CAF

CLIN	Description		Total Ceiling Price
1006	CAF	NTE	\$100,000

### ACCOUNTING FOR CONTRACTOR MANPOWER REPORTING

CLIN	Description		Total Price
1007	Accounting for Contractor Manpower Reporting		NSP

**TOTAL CEILING FIRST OPTION PERIOD CLINs:** **\$282,656,436.00**

## SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

### B.4.3 SECOND OPTION PERIOD

#### MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
2001	Labor (Tasks 1–6)	(b) (4)	(b) (4)	\$153,483,029.00

#### OPTIONAL CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
2002	Labor (Task 7)	(b) (4)	(b) (4)	\$6,164,719.00

#### COST-REIMBURSEMENT TRAVEL CLIN

CLIN	Description		Total NTE Price
2003	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	\$5,000,000

#### CPFF TOOLS, and ODC CLINs

CLIN	Description	Cost	Fixed Fee	Total NTE Price
2004	Tools Including Indirect Handling Rate (b) (4) and (b) (4) fixed fee	(b) (4)	(4)	\$52,000,000
2005	ODCs Including Indirect Handling Rate (b) (4) and (b) (4) Fee			\$65,000,000

#### CAF

CLIN	Description		Total Ceiling Price
2006	CAF	NTE	\$100,000

#### ACCOUNTING FOR CONTRACTOR MANPOWER REPORTING

CLIN	Description		Total Price
2007	Accounting for Contractor Manpower Reporting		NSP

**TOTAL CEILING SECOND OPTION PERIOD CLINs: \$281,747,748.00**

## SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

### B.4.4 THIRD OPTION PERIOD

#### MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
3001	Labor (Tasks 1–6)	(b) (4)	(b) (4)	\$153,213,140.00

#### OPTIONAL CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
3002	Labor (Task 7)	(b) (4)		\$6,287,770.00

#### COST-REIMBURSEMENT TRAVEL CLIN

CLIN	Description		Total NTE Price
3003	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	\$5,000,000

#### CPFF TOOLS, and ODC CLINs

CLIN	Description	Cost	Fixed Fee	Total NTE Price
3004	Tools Including Indirect Handling Rate (b) (4) and (b) (4) fixed fee	(b) (4)	(4)	\$52,000,000
3005	ODCs Including Indirect Handling Rate (b) (4) and (b) (4) Fee			\$65,000,000

#### CAF

CLIN	Description		Total Ceiling Price
3006	CAF	NTE	\$100,000

#### ACCOUNTING FOR CONTRACTOR MANPOWER REPORTING

CLIN	Description		Total Price
3007	Accounting for Contractor Manpower Reporting		NSP

**TOTAL CEILING THIRD OPTION PERIOD CLINs:**

**\$281,600,910.00**

## SECTION B – SUPPLIES OR SERVICES AND PRICES/COSTS

### B.4.5 FOURTH OPTION PERIOD

#### MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
4001	Labor (Tasks 1–6)	(b) (4)		

#### OPTIONAL CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee	Total CPAF
4002	Labor (Task 7)	(b) (4)		

#### COST-REIMBURSEMENT TRAVEL CLIN

CLIN	Description		Total NTE Price
4003	Long-Distance Travel Including Indirect Handling Rate (b) (4)	NTE	(b) (4)

#### CPFF TOOLS, and ODC CLINs

CLIN	Description	Cost	Fixed Fee	Total NTE Price
4004	Tools Including Indirect Handling Rate (b) (4) and (b) (4) fixed fee	(b) (4)	(4)	
4005	ODCs Including Indirect Handling Rate (b) (4) and (b) (4) Fee			

#### CAF

CLIN	Description		Total Ceiling Price
4006	CAF	NTE	(b) (4)

#### ACCOUNTING FOR CONTRACTOR MANPOWER REPORTING

CLIN	Description		Total Price
4007	Accounting for Contractor Manpower Reporting		NSP

**TOTAL CEILING FOURTH OPTION PERIOD CLINs:**

**\$218,338,454.00**

**GRAND TOTAL CEILING ALL CLINs:**

**\$1,294,982,556.00**



## **B.5 SECTION B TABLES**

### **B.5.1 LABOR OUTSIDE THE CONTINENTAL UNITED STATES (OCONUS)**

OCONUS is defined as other than the 48 contiguous states plus the District of Columbia (D.C.). The United States (U.S.) Department of State's (DoS) Bureau of Administration, Office of Allowances, publishes report indexes of living costs abroad, per-diem rate maximums, quarter's allowances, hardship differentials, and danger pay allowances. The Department of State Standardized Regulations (DSSR) is the controlling regulation for allowances and benefits available to all U.S. Government civilians assigned to foreign areas.

Contractor personnel assigned to foreign areas may receive the allowances and benefits detailed in Section H, but shall not receive allowance and benefits in excess of those identified in the DSSR.

Where costs are not specifically addressed in the DSSR, the Government will reimburse the contractor for all reasonable, allowable, and allocable costs in accordance with Federal Acquisition Regulation (FAR) 31, Contract Cost Principles and Procedures, and other applicable agency-specific regulatory supplements. The Federal Systems Integration and Management Center (FEDSIM) Contracting Officer (CO) and FEDSIM Contracting Officer's Representative (COR) will determine if costs are reasonable, allowable, and allocable.

### **B.5.2 INDIRECT/MATERIAL HANDLING RATE**

Long-Distance Travel, Tools, and ODC costs incurred may be burdened with the contractor's indirect/material handling rate in accordance with the contractor's disclosed practices, provided that the basic contract does not prohibit the application of indirect rate(s) on these costs.

- a. If no indirect/material handling rate is allowable in accordance with the contractor's disclosed practices, no indirect/material handling rate shall be applied to or reimbursed on these costs.
- b. If no rate is specified in the schedule of prices above, no indirect rate shall be applied to or reimbursed on these costs.

The indirect handling rate over the term of the TO shall not exceed the rate specified in the schedule of prices above.

### **B.5.3 DIRECT LABOR RATES**

Labor Categories (LCATs) proposed shall be mapped to existing Alliant 2 LCATs. Alliant 2 labor categories are considered bona fide executive, administrative, professional labor and generally exempt from the SCLS if used to perform professional IT services,

### **B.5.4 ACCOUNTING FOR CONTRACTOR MANPOWER REPORTING**

The costs to be reported under this CLIN are those associated with the reporting requirements specified in Section C.5.1.1 and relate to this TO only.

## **B.6 INCREMENTAL FUNDING**

### **B.6.1 INCREMENTAL FUNDING LIMITATION OF GOVERNMENT'S OBLIGATION**

Incremental funding in the amount of \$551,705,102 for CLINs 0001 through 2006 is currently allotted and available for payment by the Government. Additional incremental funding for these CLINs may be allotted and available for payment by the Government as the funds become available. The estimated Period of Performance (PoP) covered by the allotments for the mandatory CLINs is from award through June 27, 2023, unless otherwise noted in Section B. The TO may be modified to add funds incrementally up to the maximum of \$1,294,982,556 over the performance period of this TO. These allotments constitute the estimated cost for the purpose of Federal Acquisition Regulation (FAR) Clause 52.232-22, Limitation of Funds, which applies to this TO on a CLIN-by-CLIN basis.

#### **Incremental Funding Chart for CPAF**

See Section J, **Attachment C** - Incremental Funding Chart (Excel Spreadsheet).

## **B.7 AWARD FEE RESULTS REPORTING TABLE**

The Award Fee Determination Plan (AFDP) establishes award fee. See **Section J, Attachment D** – Award Fee Determination Plan (Word document).

## **C.1 BACKGROUND**

The mission of the United States Army Corps of Engineers (USACE) is to deliver vital public and military engineering services in peace and in war to strengthen the nation's security, energize the economy, and reduce risks from disasters.

USACE is a Federal agency and an Army Direct Reporting Unit made up of approximately 37,000 dedicated civilians and soldiers delivering engineering services to customers in more than 90 countries worldwide, making it the world's largest public engineering, design, and construction management agency. Reference: **(Section J, Attachment Z)** USACE Location List. USACE provides vital public services to millions of United States (U.S.) residents, and its operational capability safeguards human lives and trillions of dollars in land and private property assets. While generally associated with dams, canals, and flood protection in the U.S., USACE is also involved in a wide range of public works support to the nation and the Department of Defense (DoD) throughout the world. The USACE is the nation's number one provider of outdoor recreation and provides 24 percent of the U.S. hydropower capacity. USACE military and civilian engineers, scientists, and other specialists are also leaders of engineering and environmental missions. This diverse workforce of engineers, geologists, hydrologists, biologists, natural resource managers, and other professionals meets the demands of changing times and requirements as a vital part of the U.S. Army.

USACE provides quality, responsive engineering services to the nation, which include:

- a. Planning, designing, building, and operating water resources and other civil works projects (navigation, flood control, environmental protection, wetlands regulation, and disaster response).
- b. Designing and managing the construction of military facilities for the Army and Air Force (military construction).
- c. Providing support to the Federal Emergency Management Agency (FEMA) and other Federal, state, local, and tribal entities during national and natural Emergency Response and Recovery Operations.
- d. Surveying, acquiring, managing, condemning, and disposing of real estate for authorized Government customers.
- e. Providing design and construction management services for other Federal agencies.
- f. Planning, designing, building, and operating locks and dams. Other civil engineering projects include flood control, beach nourishment, and dredging for waterway navigation.
- g. Environmental regulation and ecosystems restoration.
- h. Maintaining more than 12,000 miles (19,000 kilometers) of commercially navigable channels across the U.S.



Figure 1. USACE Locations

### C.1.1 PURPOSE

The purpose of this requirement is to provide a modern and secure enterprise-wide IT support services to approximately 37,000 USACE customers located throughout the Continental United States (CONUS) and Outside the Continental United States (OCONUS). Services identified as part of this requirement will support the mission needs of USACE's Headquarters (HQs) located in Washington, D.C., nine Divisions (**Reference Figure 1. USACE Locations**), and 43 Districts, to include over 1,500 field and area project offices and two data centers that are currently located in Vicksburg, Mississippi, and Hillsboro, Oregon.

### **C.1.2 AGENCY MISSION**

The USACE Office of the Chief Information Officer (OCIO)/G-6 is led by the Chief Information Officer (CIO), who provides executive leadership and execution of the USACE Information Management and Information Technology (IM/IT) program.

The USACE OCIO/G-6 is composed of two primary elements: 1) the OCIO, which performs the staff functions of governance, architectural compliance and control, policy development and enforcement, portfolio management, and budget development and review; and 2) the G-6, which provides the line functions of delivering secure IM/IT services to USACE.

The OCIO/G-6 vision and direction is to be an agile, modern mission partner providing world-class IM/IT services that are secure, available, and reliable, while delivering responsive and dependable customer support exceeding expectations of USACE end users. The USACE OCIO/G-6 aims to achieve this vision by engaging mission partners and strategically forecasting future needs, to ensure desired world-class results are accomplished on time and under budget. The OCIO/G-6 seeks to support and modernize IT capabilities essential to the USACE mission through readily available, reliable, and secure network service wherever and whenever needed, as well as to continuously improve IM/IT service responsiveness and systems availability to ensure optimal customer experiences.

OCIO/G-6 provides the following enterprise-wide IM/IT services for USACE and its end users:

- a. Automation
- b. Communication
- c. Communication Security (COMSEC) Support
- d. Cyber Security (to include Information Assurance (IA))
- e. Data Center Operations Support
- f. Emergency Response
- g. Enterprise Database Management
- h. Enterprise Email Support
- i. Enterprise Service Desk
- j. Engineering Design Services for Local and Enterprise Requirements
- k. Forms Management
- l. Automated Information System (AIS) Development
- m. Personal Computer (PC) Desktop Local Support
- n. PC Lifecycle Management
- o. Print Services Liaison
- p. Project Management
- q. Publication Management
- r. Records Management
- s. Regional IT Management
- t. Service Management

## SECTION C –PERFORMANCE WORK STATEMENT

- u. Software Support
- v. Telephone (Wired and Voice over Internet Protocol (VoIP))
- w. Visual Information
- x. Video Teleconference (VTC) Support
- y. Web and SharePoint Support
- z. Wireless Device Support
- aa. Mail Peripherals
- bb. Supervisory Control And Data Acquisition (SCADA), Industrial Control Systems (ICS) and Operational Technology (OT) solutions

### **C.2 SCOPE**

The scope of the TO is to provide enterprise IT services for the USACE. The contractor shall provide technical support capabilities, including program management, IT infrastructure and shared services, general IT, cybersecurity services, engineering design, telecommunications services, emergency response, transformation, and surge/special projects capability and support. Under the oversight of and in collaboration with USACE OCIO/G-6, the contractor shall execute IT service delivery and transformation.

The contractor shall utilize Information Technology Infrastructure Library (ITIL) practices for IT Service Management (ITSM) that focuses on solutions that have an integrated, enterprise-wide focus to deliver shared IT services that align USACE OCIO/G-6 services with the needs of its customers and end users.

The places of performance for these IT services shall be at multiple locations within CONUS and OCONUS (e.g., the territories of Guam, the Virgin Islands, and Puerto Rico, and Korea, Japan, and Germany).

### **C.3 CURRENT INFORMATION TECHNOLOGY (IT) NETWORK ENVIRONMENT**

USACE OCIO/G-6 is responsible for over 130,000 IT systems, governed by a variety of management controls including Investment Review Boards and Change Control Boards. These systems are diverse and have often been tailored to meet the Government's requirements.

USACE's current environment includes approximately 20,750 servers, network devices, firewalls, appliances, and printers; 32,900 VOIP devices; 40,000 laptops, tablets, and workstations; approximately 60,000 telephone numbers and telephones; 13,000 mobile devices; Supervisory Control and Data Acquisition (SCADA) and Operational Technology (OT) equipment; and other end-user devices. The total number of devices supporting mobility is expected to slowly increase over time. Reference: **(Section J, Attachment Y)** USACE Hardware and Software List.

There are approximately 2.5 million Internet Protocol (IP) addresses across three class B networks plus some smaller networks on a continuous basis using network access control tools. These networks and devices are distributed across approximately 1,650 different locations and sites.

## SECTION C –PERFORMANCE WORK STATEMENT

The contractor shall seamlessly assume the current USACE environment to maintain and operate existing systems. After Task Order Award (TOA), the contractor shall work with the Government to begin the transformation process.

USACE OCIO/G-6 currently utilizes Microsoft (MS), Amazon Web Services (AWS), and Oracle cloud services and intends to increase cloud presence during performance of this TO

The strategic USACE OCIO/G-6 IT direction will shift IT delivery from a decentralized, primarily Government-owned, contractor-operated, stove-piped approach to a business model that has an integrated, enterprise-wide focus supporting a mix of Government-owned, contractor-operated and contractor-owned, contractor-operated environments. This model employs a portfolio-based approach that delivers shared services using an established governance structure.

### **C.4 OBJECTIVE**

The objective of this TO is to assist the USACE OCIO/G-6 with its goals by providing agile, innovative, customer-focused and cost-effective integrated enterprise IT support services in support of USACE's mission of engineering solutions for the nation's toughest challenges. This TO shall provide enterprise IT solutions to enhance and strengthen USACE's IT foundation and deliver secure, revolutionary, and modernized technological solutions to end users and customers.

The proposed strategic USACE OCIO/G-6 IT direction will shift IT delivery from a decentralized, stove-piped approach to a business model that has an integrated, enterprise-wide focus including contractor-owned, contractor operated solutions as recommended by the contractor and approved by the Government. This model employs a portfolio-based approach that delivers shared services using an established governance structure.

USACE OCIO/G-6 is aligning its IT capabilities to provide enterprise service delivery and evolve infrastructure and service delivery from its current state to a modern service delivery model. This new model will increasingly rely on contractor-provided devices and infrastructure to enhance the end-user experience and to support the vital USACE mission of delivering engineering solutions.

The contractor shall provide integrated, consumption based, IT support services for the USACE enterprise bolstering the end-user experience. The contractor shall leverage technology and business processes to build synergies across the enterprise, develop and maintain consistency in process and procedures, and increase mission capabilities of USACE end users.

The contractor shall support USACE OCIO/G-6 through successful performance of the following high-level objectives:

- a. Continual modernization of USACE's portfolio of IT systems and ensure USACE remains a leader in cybersecurity compliance, positive audit results, patching speed, and security innovation.
- b. Deliver enterprise-wide IT solutions that are well-integrated, flexible, and adaptable across all IT service areas, with the ability to rapidly scale in response to USACE dynamic business environment.

## SECTION C – PERFORMANCE WORK STATEMENT

- c. Support a geographically dispersed workforce and deploy greater coverage at remote sites to increase the use of real-time tools. USACE seeks to modernize its IT systems and infrastructure by providing field offices with upgraded IT support.
- d. Develop a balance between delivering tactical support (operations and maintenance) and strategic support (development, modernization, and enhancement) that achieves operational and cost efficiencies while positioning USACE stakeholders and end users to fulfill their mission.
- e. Deploy IT services appropriately to the identified need with the ability to apportion charges to internal and external clients according to use. (A functioning, equitable, and transparent service charge-back mechanism in place across the enterprise.)
- f. Maintain a secure environment that includes necessary authorization and authentication, which adequately protects privacy information.
- g. Provide service cost and other service management details to ensure USACE remains a leader in technology management, exceeding the expectations set forth by the Office of Management and Budget's (OMB's) annual Federal Information Security Management Act (FISMA) objectives, as well as providing cost transparency to the USACE CIO G/6 customer base.

### **C.5 TASKS**

- a. Task 1 – Program Management
- b. Task 2 – Enterprise Shared Services
- c. Task 3 – General IT Support
- d. Task 4 – Cybersecurity
- e. Task 5 – Telecommunications
- f. Task 6 – Transformation
- g. Task 7 – Emergency Response (Optional)

#### **C.5.1 TASK 1 – PROGRAM MANAGEMENT SUPPORT**

The contractor shall provide program management support under this requirement. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS).

The contractor's governance structure shall be scalable to effectively support an enterprise environment: defined as a singular organization derived from multiple funding entities with the need to separately track project management and contract elements such as requirements, deliverables, costs, and ceiling. The Government will utilize the term Technical Direction Letter (TDL) to identify and track operational support needs. These TDLs will be initiated at varying times within the PoP, vary from enterprise-wide to local site requirements, and consist of various appropriation types (e.g., one-year, two-year, no-year, etc.) depending on the bona fide need. These efforts are severable in nature, impacting the level of tracking required to ensure that the Government maximizes the availability of funds.



**C.5.1.1 SUBTASK 1 – ACCOUNTING FOR CONTRACTOR MANPOWER REPORTING**

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this Contract for the USACE. The contractor shall completely fill in all required data fields using the following web address: <http://www.sam.gov>.

Reporting inputs shall be for the labor executed during the PoP during each Government Fiscal Year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the support desk at: <http://www.sam.gov>.

**C.5.1.2 SUBTASK 2 – COORDINATE A PROGRAM KICK-OFF MEETING**

The contractor shall schedule, coordinate, and host a Program Kick-Off Meeting at the location approved by the Government (**Section F, Deliverable 01**). The meeting shall provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting shall provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include Key contractor Personnel, representatives from the directorates, the USACE Technical Point of Contact (TPOC), other relevant Government personnel, and the FEDSIM COR.

At least three days prior to the Kick-Off Meeting, the contractor shall provide a Kick-Off Meeting Agenda (**Section F, Deliverable 02**) for review and approval by the FEDSIM COR and the USACE TPOC prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

- a. Introduction of team members and personnel to include roles, responsibilities, and lines of communication, including Points of Contact (POCs), between the contractor and the Government.
- b. Staffing Plan and status.
- c. Transition-In Plan (**Section F, Deliverable 03**) and discussion.
- d. Security discussion and requirements (i.e., building access, badges, Common Access Cards (CACs)).
- e. Financial forecasting/tracking and invoicing requirements
- f. TDL management process.
- g. Project Management Plan (PMP) discussion including schedule, tasks, etc.
- h. Baseline Quality Management Plan (QMP) (**Section F, Deliverable 04**).
- i. Service Integration and Management (SIAM) plan (**Section F, Deliverable 05**).
- j. Cyber Security Management Plan (CSM) (**Section F, Deliverable 06**)
- k. Proposed Task Order (TO) Portal (**Section F, Deliverable 07**)

## SECTION C – PERFORMANCE WORK STATEMENT

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting, and the contractor shall provide sufficient copies of the presentation for all present.

The contractor shall draft and provide a Kick-Off Meeting Minutes Report (**Section F, Deliverable 08**) documenting the Kick-Off Meeting discussion and capturing any action items.

### **C.5.1.3 SUBTASK 3 – PROGRAM MANAGEMENT REVIEW (PMR)**

The contractor shall develop and provide a monthly PMR (**Section J, Attachment F**) (**Section F, Deliverable 09**). The PMR shall include the following:

- a. Activities during reporting period, by task (include ongoing activities, new activities, and activities completed, and progress to date on all above mentioned activities) by TDL. Each section shall start with a brief description of the task.
- b. Report system outages and impact on uptime/availability percentages.
- c. Report services' performance outside of tolerance thresholds.
- d. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
- e. Updated Personnel Roster that includes all contractor personnel (including subcontractors and teaming partners) by location, project, ALLIANT 2 labor category, and functional role. The roster shall also specifically identify any gains, losses, and status changes (e.g., security clearance).
- f. Government actions required.
- g. Schedule (show major tasks, milestones, and deliverables, and planned and actual start and completion dates for each).
- h. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the PMR for reporting period).
- i. Detailed cost accounting by CLIN, Task, Subtask, ACE Work Center and/or TDL.
- j. Costs incurred by CLIN, Task and Subtask, ACE Work Center and/or TDL Costs incurred but not billed by CLIN, Task and Subtask, ACE Work Center and/or TDL
- k. Accumulated invoiced cost for each CLIN, Task, Subtask, ACE Work Center and/or TDL up to the previous month.
- l. Estimate at completion for each CLIN, Task and Subtask, ACE Work Center and/or TDL
- m. Variance at completion based on funding availability for each CLIN, Task and Subtask, ACE work Center and/or TDL.
- n. Updates for USACE CIO/G6 service areas supported

The contractor Program Manager (PM) shall convene a monthly Program Review Meeting with the USACE TPOC, FEDSIM Contracting Officer's Representative (COR), and other Government stakeholders (**Section F, Deliverable 10**). The purpose of this meeting is to ensure all stakeholders are informed of the technical monthly activities and PMR, provide opportunities to identify other activities and establish priorities, provide updates on program financials and identify any financial issues, and coordinate resolution of identified problems or opportunities.

## SECTION C – PERFORMANCE WORK STATEMENT

The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the FEDSIM COR (**Section F, Deliverable 11**).

### **C.5.1.4 SUBTASK 4 – CONVENE TECHNICAL EXCHANGE MEETINGS**

The contractor shall convene Technical Exchange Meetings with individual service-level components and other Government stakeholders as required. The Technical Exchange Meetings shall provide an opportunity for the contractor and service-level components to review the status of services being provided. The contractor shall provide minutes of these meetings when requested by the Government, including attendance, issues discussed, decisions made, and action items assigned, to the USACE TPOC and FEDSIM COR within two workdays following the meeting (**Section F, Deliverable 12**).

### **C.5.1.5 SUBTASK 5 – PREPARE AND UPDATE A PROJECT MANAGEMENT PLAN (PMP)**

The contractor shall document all support requirements in a PMP and shall provide it to the Government (**Section F, Deliverable 13**).

The PMP shall:

- a. Describe the proposed management approach.
- b. Contain detailed Standard Operating Procedures (SOPs) for TO tasks and service delivery.
- c. Include milestones, tasks, and subtasks required in this TO.
- d. Provide for an overall Work Breakdown Structure (WBS).
- e. Describe in detail the contractor's approach to risk management under this TO.
- f. Describe in detail the contractor's approach to communications, including processes, procedures, and other rules of engagement between the contractor and the Government.
- g. Contain a Communication Plan to identify and track all required communications as part of the PMP, which identifies all key stakeholders and appropriate communications formats (e.g., meetings and briefings), content, and schedules for each stakeholder.
- h. Include the contractor's QMP.
- i. Include the contractor's Accident Prevention Plan as identified in H.24 Accident Prevention Plan

The PMP is evolutionary documents that shall be updated annually at a minimum and as project changes occur. The contractor shall work from the latest Government-approved version of the PMP.

### **C.5.1.6 SUBTASK 6 – PREPARE TRIP REPORTS**

The Government will identify the need for a Trip Report when the request for travel is submitted (**Section F, Deliverable 14**). The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and

POC at travel location. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any knowledge gained. At a minimum, trip reports shall be prepared with the information provided in **Section J, Attachment G**.

#### **C.5.1.7 SUBTASK 7 – PROVIDE QUALITY MANAGEMENT**

The contractor shall identify and implement its approach for providing and ensuring quality throughout TO performance. The contractor shall provide a QMP and maintain and update it as changes in the program processes are identified (**Section F, Deliverable 04**). The contractor's QMP shall describe the application of the appropriate methodology (i.e., quality control and/or quality assurance) for accomplishing TO performance expectations and objectives. The QMP shall describe how the appropriate methodology integrates with the Government's requirements.

#### **C.5.1.8 SUBTASK 8 – TRANSITION-IN**

The contractor shall provide transition-in services for the TO. The contractor shall execute a two-phased transition process as outlined in **Section J, Attachment AA**. The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. The contractor shall conclude all transition-in activities no later than 180 calendar days after TOA.

The contractor shall provide a Transition-In Plan (**Section F, Deliverable 03**) for Government approval that shall address the Tasks in Section C.5, identifying the roles and responsibilities of the contractor and any incumbent contractor(s) (if applicable), information expected from the incumbent contractor(s) (if applicable), the process to ensure that current vital USACE activities that are within scope of the TO are continued without disruption, a draft schedule(s), to include the anticipated timeline for appropriate personnel security processing, and milestones to ensure no disruption of Government service during and after the transition-in period.

The Transition-In Plan shall document how the contractor plans to seamlessly transition all existing services from the current provider(s), add new services, and minimize operational and project impacts. At a minimum, the Transition-in Plan shall include:

- a. Transition schedule with tasks, duration, milestones, resource allocation, knowledge transfer sessions, and dates for completion of work transfer from current provider(s) to contractor.
- b. Plan sections dedicated to the transition of Operational and Service Desk support with emphasis on integration with the outgoing provider and obtaining system access to support seamless hand-off of responsibilities.
- c. Contractor onboarding plan and schedule that considers time to initiate background investigations and receive initial enter on duty determination to obtain access card, network and email account, and complete USACE-required training.
- d. Summary and schedule for Government-Furnished Information (GFI), Government-Furnished Equipment (GFE), and space.

## SECTION C – PERFORMANCE WORK STATEMENT

- e. Schedules for Transition-In Progress Reviews (IPR), Status Reports, and Operational Readiness Review(s).
- f. Risks and associated risk mitigation plans.

The contractor shall implement its Government-approved Transition-In Plan No Later Than (NLT) fifteen calendar days after the TO Kick-Off Meeting. Phase One transition activities shall be completed 90 calendar days from TOA with the contractor achieving full operational performance for the task identified in **Section J, Attachment AA**. Phase Two transition activities shall be completed 180 calendar days after TOA with the contractor achieving full operational performance for tasks as identified in **Section J, Attachment AA** 140 calendar days after approval of the Transition-In Plan (**Section F, Deliverable 03**) but NLT 180 calendar days from TOA.

### **C.5.1.9 SUBTASK 9 – TRANSITION-OUT**

The contractor shall provide transition-out support when required by the Government. The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a Transition-Out Plan within six months of Project Start (PS) (**Section F, Deliverable 15**). The contractor shall review and update the Transition-Out Plan in accordance with the specifications in **Sections E and F**.

In the Transition-Out Plan, the contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

- a. Project management processes.
- b. POCs.
- c. Location of technical and project management documentation.
- d. Status of ongoing technical initiatives.
- e. Appropriate contractor-to-contractor coordination to ensure a seamless transition.
- f. Transition of Key Personnel.
- g. Schedules and milestones.
- h. Asset Inventory identifying Contractor or Government ownership.
- i. Actions required of the Government.

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless transition-out.

The contractor shall implement its Transition-Out Plan NLT six months prior to expiration of the TO.

### **C.5.1.10 SUBTASK 10 – SERVICE INTEGRATION AND MANAGEMENT (SIAM)**

Support services will be segmented between the Government and the contractor, and other service providers. The Government requires the contractor's approach to SIAM to provide

## SECTION C –PERFORMANCE WORK STATEMENT

coordination of multiple service providers with the goal of seamlessly integrating interdependent services from various internal Government and external service providers into efficient, innovative, agile, and cost-effective, end-to-end services that meet USACE mission needs.

The contractor shall act as the primary service integrator for IT related services. The Government will act as the primary Service Integrator (SI) for other services and for integration, as needed, between the contractor and other service providers.

The contractor shall document all support requirements in a SIAM Plan and shall provide it to the Government (**Section F, Deliverable 05**) at the Kick-Off meeting. The SIAM Plan is an evolutionary document that shall be updated annually at a minimum and as program changes occur. The contractor shall work from the latest Government-approved version of the Plan.

### **C.5.1.11 SUBTASK 11 – IMPLEMENT A TASK ORDER (TO) MANAGEMENT PORTAL**

The objective of the TO management portal is to introduce efficiencies and ensure coordinated service delivery and provide a central location for the Government and contractor to access management-level information regarding the status and health of TO activities.

The contractor shall implement and maintain a secure, web-based portal capability that provides program management views/reporting, tracks metrics, and stores artifacts at the unclassified level. Government-approved contractor personnel and Government personnel shall have access to the portals worldwide. The portal shall be Common-Access Card (CAC) or Personal Identity Verification (PIV) enabled to allow users with either a CAC or PIV credential access. The portal content shall be maintained and revised throughout the duration of the TO. The contractor shall implement cybersecurity best practices to protect the portal system and data contained within the portal.

At a minimum, the portal shall provide the following:

- a. Secure logical access controls with user-based views.
- b. A dashboard that identifies each TDL being supported:
  1. Customer POC and entity.
  2. Lead contractor POC information.
  3. Project duration.
  4. Applicable schedule information.
  5. Allocated budget by CLIN.
  6. Funded amount by CLIN.
  7. Incurred cost amount by CLIN.
  8. Invoiced amount, invoice number and date(s).
- c. A staffing roster inclusive of name, TDL, functional role, location, and clearance level.
- d. An automated workflow for Government review/approval of RIPs/CTPs, TARs, deliverables, and TDLs, inclusive of the USACE TPOC and FEDSIM COR.

## SECTION C – PERFORMANCE WORK STATEMENT

- e. The ability to view financial information to allow the Government to track financial health. The Government will establish the level of granularity needed at the onset of an effort (funding document, ACE Work Center or line of accounting level).
- f. Financial reporting capabilities to meet USACE OCIO/G-6 resource management requirements, to include Technology Business Model (TBM) and the tracking of expenses to the lowest activity level.
- g. An organized document library to store management-related deliverables (e.g., monthly reports, meeting minutes, financial reports, PMP, etc.)
- h. The contractor's portal solution shall provide and maintain an enterprise IT services dashboard. The dashboard shall provide automated and Government-accessible, enterprise-wide metrics, statistics, and real-time data on critical success factors and key performance indicators regarding the provisioning of IT services to support performance management objectives and decisions on the investment and management of IT resources. The contractor shall maintain, in a readily accessible and easy-to-use format, the capability to display (report) information critical to the USACE OCIO/G-6 and customer base on an enterprise-wide basis including, but not limited to: system outages, application issues, cybersecurity information, call-center statistics, health and performance of critical IT services, and status of service desk tickets. The dashboard shall allow OCIO/G-6 to query information, generate custom reports, and conduct data fusion.
- i. Risk management information, including identification of risks, severity, and extent, identification of security tool effectiveness, and risk-based prioritization of efforts.
- j. Lessons learned database to assist with process improvement projects.
- k. Results of assessment or audit, including pre-audit, during, and after audit assessments.
- l. Telecommunications management information, including expense management.
- m. Task reporting and approval capability, to track internal USACE OCIO/G-6 tasks and packets for approval and execution.

The contractor shall deliver a proposed portal solution at the TO Kick-Off Meeting (**Section F, Deliverable 07**) for approval from the FEDSIM COR. The contractor shall implement and have its portal solution fully operational by 90 calendar days after TOA. The portal capabilities are expected to evolve and adapt to meet the mission needs of the Government.

### **C.5.1.12 SUBTASK 12 – IT GOVERNANCE**

Governance is a necessary component for ensuring effective integration of enterprise-wide IT services into the USACE environment. The contractor shall provide IT governance services to identify cost and other service management details to ensure USACE remains a leader in technology management, exceeding the expectations set forth by OMB's annual objectives, as well as providing cost transparency to the USACE OCIO/G-6 customer base. The contractor shall ensure compliance with all applicable (e.g., Federal, DoD, Army, OMB, USACE, etc.) regulations and policy during TO performance.

The contractor shall provide USACE IT Governance Documentation (**Section F, Deliverable 16**) that shall assist USACE OCIO/G-6 and USACE stakeholders, customers, and end users with

strengthening and enhancing USACE OCIO/G-6's IT operating environment. Governance documentation shall be submitted to USACE OCIO/G-6 for review and approval.

The contractor shall review proposed changes to Government IT policies, architectures, standards, and procedures, and recommend additions, modifications, and deletions as needed to satisfy governance requirements. The contractor shall advise the Government of any adverse impacts to stability, cost, architecture, interoperability, compatibility, and service and recommend mitigation strategies. Governance of the IT services delivered to USACE is a significant effort requiring a joint commitment from the Government governance teams and the contractor governance teams.

**C.5.1.13 SUBTASK 13 – PREPARE AND UPDATE TECHNICAL DIRECTION PLAN(S) (TDPs)**

The Government anticipates that this will be a project-based TO with multiple projects operating concurrently among the USACE organizations. Work within the scope and tasks of the TO will be directed by USACE OCIO/G-6, TDL, in accordance with H.15, initiated by the Government and completed by the contractor in the form of a Technical Direction Plan (TDP). The FEDSIM CO will provide written confirmation and approval that each TDP is within the TO scope of requirements. The contractor shall provide all expertise and services as stated in the TO to deliver the integrated professional services.

TDLs will be initiated at varying times within a PoP, consisting of various appropriation types (e.g., one-year, two-year, or no-year), depending on the bona fide need.

In response to the Government's TDL, the contractor shall provide, at a minimum, the following information as part of a TDP:

- a. Summary of the Government's requirements that includes, at a minimum, the project specifications, structure, activities, conditions, risks, mitigations, and schedule from project inception through project closeout. All project milestones shall be detailed with clear, unambiguous target dates.
- b. Project staffing and resource profile.
- c. Travel and ODC considerations.
- d. Security considerations.
- e. Detailed project cost estimate broken out by CLIN.

Once the TDP (**Section F, Deliverable 17**) has been approved by the FEDSIM CO and FEDSIM COR, the contractor shall schedule and coordinate a TDP Kick-Off Meeting (**Section F, Deliverable 19**) at a location approved by the Government if required. Project Kick-Off Meetings may be held virtually pending approval from the FEDSIM COR. The meeting shall provide an introduction between the contractor personnel and Government personnel who will be involved with the project. The meeting shall provide the Government and the contractor with an opportunity to discuss technical, management, and security issues as well as other TO processes and procedures. At a minimum, the attendees shall include the contractor PM, relevant Government representatives, the USACE OCIO/G-6 TPOC, and the FEDSIM COR.



## SECTION C –PERFORMANCE WORK STATEMENT

Prior to the TDP Kick-Off Meeting, the contractor shall provide a TDP Kick-Off Meeting Agenda (**Section F, Deliverable 19**) for review and approval by the FEDSIM COR and the USACE OCIO/G-6 TPOC prior to finalizing. The agenda shall include, at a minimum, the following topics:

- a. Introduction of team members and personnel including roles, responsibilities, and lines of communication between the contractor and the Government.
- b. Discussion of the TDL requirements.
- c. Discussion of the cost estimate.
- d. Discussion of staffing and status.

The contractor shall draft and provide a TDP Kick-Off Meeting Minutes Report (**Section F, Deliverable 20**) documenting the TDP Kick-Off Meeting discussion and capturing any action items.

Following the project Kick-Off Meeting, the contractor shall provide the updated TDP (**Section F, Deliverable 17**) to the FEDSIM CO and FEDSIM COR for review and approval in accordance with Section E. The TDP is an evolutionary document that shall be updated, at a minimum, annually or as changes occur or the project reaches completion (**Section F, Deliverable 17**). The contractor shall work from the latest Government-approved version of the TDP. In the event there is a conflict between the TDL and the TO, the TO shall always take precedence. The FEDSIM CO will approve all changes.

Following the project completion, the contractor shall provide a signed Project Closeout Form (**Section F, Deliverable 18**) documenting the project closeout action items.

### **C.5.2 TASK 2 – ENTERPRISE SHARED SERVICES**

USACE OCIO/G-6 requires infrastructure and shared services, including the day-to-day operational activities required of the contractor to provide end-to-end, enterprise-level monitoring, management, administration, performance optimization, and maintenance for all IT services, devices, applications, and infrastructure. The contractor shall support physical devices and software applications inclusive of hardware, software, networks, and facilities that are required to develop, test, deliver, monitor, control, purchase, or support IT services necessary to operate the entire enterprise. The contractor shall support USACE's current operations by performing assessments, submitting recommendations, and executing phased service implementations to migrate IT to as-a-service models or improve current state where appropriate and approved by USACE CIO (**Section F, Deliverable 21**).

Enterprise shared services are IT services and procurements that are common among USACE operating units.

#### **C.5.2.1 SUBTASK 1 – MANAGED SEAT SERVICES**

The contractor shall provide IT services to all supported CONUS and OCONUS locations. Services shall be provided in accordance with standard approaches, such as ITIL current version, Configuration Maturity Model Integration (CMMI) for development, CMMI services,

## SECTION C –PERFORMANCE WORK STATEMENT

International Organization for Standardization (ISO)/International Electro technical Commission IEC 20000-1:2011, ISO/IEC 27001, or a comparable service delivery methodology. The Revolutionary Information Technology Services (RITS) contractor shall assume the current IT environment initially utilizing existing, Government-owned devices to the most practical extent, and then phase in revised solutions based on Government-approved transformations.

The contractor shall:

- a. Provide zero or thin client, desktop, laptop, and high-performance end-user computing services and peripheral devices to approved USACE employees.
- b. Provide remote access capability for all seat service end users in the CONUS and OCONUS.
- c. Provide comprehensive customer service, including remote support, deskside support (as required), self-service, and walk-up service to ensure continued productivity of end users.
- d. Provide access to customer support through a wide variety of channels including email, internet, chat, and telephone.
- e. Provide identity, credential, and access management services.
- f. Provide capability for handling the day-to-day logistics of deploying integrated solutions, including, but not limited to, ordering, scheduling, provisioning, imaging, patching, securing, sanitizing, testing, tracking, distribution, storage, and transportation of assets.
- g. Provide onboarding solutions to allow new employees to complete USACE IT onboarding requirements efficiently.

### **C.5.2.2 SUBTASK 2 – PRINT SERVICES**

#### **C.5.2.2.1 BASIC PRINT SERVICES**

The contractor shall provide each USACE division, basic print services for all devices identified, and will be required to operate, install, configure, and maintain printer devices, including printers, fax machines, copiers, scanners, postage meters, and plotters. The contractor shall maintain the device inventory. The Government will provide and install paper, toner, or ink cartridges.

#### **C.5.2.2.2 MANAGED PRINT SERVICES**

The contractor shall provide managed print services when requested by any USACE division in accordance with the TDL process specified in **Section H.15**. Managed print services are completed in lieu of basic print services, and the contractor TDL shall only identify increases in labor and cost above that required by basic print services (**Section C.5.2.2.1**). The contractor shall analyze the printing needs of the division and provide the appropriate devices in a COCO model to optimize efficiency and minimize costs. Devices include printers, fax machines, copiers, scanners, postage meters, and plotters. The contractor shall be solely responsible to ensure devices are operational at all times and shall be solely responsible for all repairs and device replacements. The contractor shall maintain the device inventory and provide paper, toner, or ink cartridges.

### **C.5.2.3 SUBTASK 3 – UNIFIED COMMUNICATIONS (UC) SERVICES**

USACE requires UC services to integrate communication platforms and optimize the end-user experience. The contractor shall provide a best-in-class UC service, recommend improvements and enhancements to the Government, and execute successful upgrades and transitions when requested and approved by the Government. The contractor shall provide VTC, audio/visual, and telepresence support, including training, set-up, maintenance, troubleshooting, and repair. Additionally the contractor shall support, manage, and ensure operability of USACE communications systems that operate on analog or digital connectivity (Private Branch Exchange (PBX), fax machines, Public Switched Telephone Network (PSTN), Plain Old Telephone Service (POTS) lines etc.).

#### **C.5.2.3.1 VIDEO TELECONFERENCE (VTC) SERVICES**

The contractor shall provide core UC VTC services and audio/visual and telepresence support and expertise to ensure successful VTC operation by USACE end users. Required services include, but are not limited to, training end users on how to use equipment; placement, set-up, maintenance, testing, and troubleshooting of equipment; and completing repairs necessary to ensure proper operation of all equipment in conference rooms, training rooms, auditoriums, offices, workspaces, and telepresence rooms.

Any inoperable VTC equipment shall be repaired or replaced by the contractor. All facets and components of the VTC system are the responsibility of the contractor.

The contractor shall provide VTC-hosting capability to support VTC connections by multiple simultaneous participants, including conference room and desktop VTC systems containing both internal and external connections. The contractor shall configure and maintain the entire existing audio conferencing and VTC system, including the IP bridge and registered systems directory.

The Government will order via the TDL process identified in **Section H.15** on site support services as required. The contractor shall provide capability for an on-site and in-person contractor presence for live troubleshooting and support of classified (Secret) and non-classified meetings. Additionally, the contractor shall support live streaming of meetings and events when requested.

#### **C.5.2.3.2 INTERNET PROTOCOL (IP) VOICE SERVICES**

The contractor shall provide core UC IP voice services, including training end users on how to use equipment and the procurement, placement, set-up, maintenance, and compliance verification of equipment, inclusive of testing, troubleshooting, and completing repairs necessary to ensure proper operation of all IP voice equipment in conference rooms, training rooms, auditoriums, offices, workspaces, and telepresence rooms. Any inoperable IP voice equipment shall be repaired or replaced by the contractor. All facets and components of the IP voice system are the responsibility of the contractor. Additionally, the contractor shall provide support services for the installation, operation, and management of UC software that enables end users to manage IP voice service from either their computer or their IP voice equipment, and 911 location services in accordance with the DoD Policy Reference Ray Baum's Act of 2018, H.R. 4986,

115th Congress (2018), identifying the area of building and floor for emergency response providers in emergency situations.

#### **C.5.2.4 SUBTASK 4 – INFRASTRUCTURE SUPPORT SERVICES**

USACE OCIO/G-6 requires infrastructure support services to continually align enterprise IT capabilities with USACE’s evolving cloud migration strategy. This shall ensure the IT service delivery can effectively support the current and future IT requirements of USACE OCIO/G-6, customers, and end users.

The contractor shall assume responsibility for the current, Government-owned, end-user environment and implement a contractor’s lifecycle management plan for maintenance of OCIO/G-6 supported infrastructure. Contractor-provided services shall include managing and maintaining existing infrastructure (UNIX/LINUX/AIX/Windows Servers) and ensuring legacy IT systems and business applications operate seamlessly with contractor-provided services, installation, configuration, maintenance, upgrades, and version currency and refresh of infrastructure and devices. Contractor-provided operations and maintenance of USACE infrastructure requires capacity for changes in technology or reconfiguration as a result of the business environment.

During TO performance the contractor shall support USACE’s cloud smart migration strategy, including providing scalable, metered solutions capable of supporting USACE’s application and data storage needs, to include Datacenter-as-a-Service (DCaaS), Federal Risk and Authorization Management Program (FedRAMP), and DoD Provisional Authority (PA)-authorized commercial cloud capabilities. The contractor’s cloud solution shall scale compute capabilities appropriately in terms of central processing unit processing power, available memory, and available storage space, to accommodate surges in usage or data. The contractor shall ensure all DCaaS service needs are adequately provided including, but not limited to, cooling, power supply, server components, backups, Disaster Recovery (DR), bandwidth, capacity, and storage. The contractor shall support existing data center cloud and future cloud migration strategy. The contractor shall continually provide performance optimization and remediate degradation, performance analysis, baseline, monitoring, alerting, root cause analysis and remediation, and continuous improvement proposals.

#### **C.5.2.5 SUBTASK 5 – INTERNAL AND EXTERNAL CAMPUS CONNECTIVITY**

USACE is continually updating bandwidth to meet mission needs of operating divisions. As a result, service distribution methods such as switching to fiber from coaxial cable may be required. USACE requires the contractor to develop, plan, and implement innovative turnkey, connectivity solutions for campus environments, including building-to-building connectivity for non-standard locations such as hydroelectric stations, parks, locks, and dams. All designs and implementations shall be in accordance with DoD, USACE, and industry standards and best practices where DoD and USACE standards do not currently exist. Coordination with local facilities for on-site support may be required.

## SECTION C –PERFORMANCE WORK STATEMENT

The contractor shall develop, plan, implement, and/or review others' plans for a structured turnkey inside-plant, cabling solution that will support wired and wireless voice, data, and video services to the desktop (**Section F, Deliverable 22**). This solution shall support the USACE mission at all USACE sites, including, but not limited to, HQ, districts, divisions, field sites, vessels, military installations, and remote locations. The contractor shall provide these services as required and identified by local government IT personnel.

### **C.5.2.6 SUBTASK 6 – NETWORKING**

The contractor shall provide network infrastructure services. For each of the below services, the contractor shall engage in continuous troubleshooting, evaluation, and improvement of capabilities to provide a continuously improving network environment.

The contractor shall provide and maintain a Network Operations and Security Center (NOSC) capability in accordance with DoD Instruction (DoDI) 8530.01 and Army Regulation (AR) 25-1, incorporating all facets of a Security Operations Center (SOC), and a Network Operations Center (NOC). The contractor-provided NOSC shall support network communications, including data, voice, and video services, at USACE locations throughout the CONUS and OCONUS locations, provide continuous (24 hours per day, seven days per week, 365 days per year (24/7/365)) network performance monitoring, incident detection, network security functions, and problem resolution. The NOSC shall perform the dual roles as one entity maintaining a high degree of communication with service owners.

The contractor shall provide managed Wide Area Network (WAN), Metropolitan Area Network (MAN) and managed Local Area Network (LAN) services, encompassing access layer, distribution layer, and network core components.

### **C.5.2.7 SUBTASK 7 – ENTERPRISE IT SERVICE DESK**

The service desk shall provide support to users of USACE's internal infrastructure, applications, systems, and devices (including end-user devices and mobile devices) utilized by USACE. The service desk shall be the single POC for USACE end users and customers for all IT areas, applications, and business processes to report incidents; submit service requests; seek advice; obtain training; request hardware, mobile devices, or software; and register complaints about USACE's IT infrastructure, devices, applications, and programs supported in the environment. The service desk shall aggressively identify root causes impacting customer experience and work to eliminate all recurring issues identified as detrimental to overall service levels. Furthermore, the service desk shall support USACE by identifying system bottlenecks and developing mitigation and action plans to correct system performance issues.

The service desk shall also provide an interface for users to access other service management functions, such as, but not limited to, requests for services, change management, problem management, configuration management, and release management. The service desk shall use a tracking solution for all incoming incidents; provide automated ticket tracking, routing, escalation and email notifications; provide basic incident and service request management; and

display basic self-service options for end users. The contractor shall provide service desk support that shall support remote end users 24/7/365 and cover classified and unclassified systems.

### **C.5.3 TASK 3 – GENERAL IT SUPPORT**

General IT support includes monitoring and maintaining USACE databases and systems, completing installs, configuring hardware and software, and solving technical problems.

#### **C.5.3.1 SUBTASK 1 – DATABASE SUPPORT**

The design, development, management, inclusive of migration and optimization, enhancement, and sustainment of data and databases in the USACE OCIO/G-6 portfolio of systems are critical to the USACE mission. The contractor shall:

- a. Administer databases and related components to include incorporating changes or updates.
- b. Provide continuous improvement to existing databases to include the integration of the information within the database to facilitate data sharing across the applications.
- c. Adhere to current Government data standards.

#### **C.5.3.2 SUBTASK 2 – SYSTEMS ENGINEERING**

The contractor shall provide a Systems Engineering Management Plan (SEMP) (**Section F, Deliverable 23**). In support of USACE systems engineering, the contractor shall:

- a. Identify customer and stakeholder needs.
- b. Capture and evaluate customer requirements.
- c. Design, build, test, and deploy solutions to meet customer requirements.
- d. Analyze the impact of emerging technologies on current strategies and develop a vision for the technological future of USACE.
- e. Track the alignment of IT and information management trends with USACE mission requirements and influence the deployment of technology.
- f. Lead activities to investigate, plan, and manage the deployment of products and services into the USACE operating environment; address IT performance gaps and technology overlaps throughout the USACE operating environment.
- g. Conduct technology feasibility assessments.
- h. Utilize commercially available tools to establish performance baselines, monitor systems performance against established baselines, identify performance issues, and develop and implement solutions to enhance and maximize system performance in accordance with the contractor's approved SEMP.
- i. Conduct comprehensive evaluations of technology solutions and document findings in the appropriate repository of record.
- j. Support the establishment and management of an enterprise engineering service brokerage model to ingest customer requests, define requirements, and prioritize,



resource, schedule, and execute engineering services using standardized processes and procedures.

- k. Provide expert knowledge and skill in planning and designing engineering solutions required to support systems engineering and integration efforts integrated with cyber security to meet customer requirements.
- l. Produce associated documentation requirements, templates for deliverable artifacts, forms, and checklists.

#### **C.5.3.3 SUBTASK 3 – WEBSITE DEVELOPMENT**

The contractor shall support USACE personnel with website development that accurately reflects USACE messaging and promotes the strategic objectives of USACE communications. The contractor shall ensure that all public-facing websites and content are in compliance with USACE's Public Affairs (PA) website standards to ensure a consistent appearance and style. The contractor shall support activities to ensure the registration and vulnerability assessments of websites are performed prior to promotion and lifecycle management has been engaged for the site.

#### **C.5.3.4 SUBTASK 4 – END-USER TRAINING**

In conjunction with the administration, development, release, or replacement of enterprise-level initiatives, the contractor shall assess end user training needs, develop a Training Plan (**Section F, Deliverable 24**) and deliver training required for end users. The contractor shall maintain repositories of training documentation in formats widely accessible to stakeholders. The contractor shall provide a solution for end users to provide feedback on training taken in order to continually monitor and improve subsequent trainings.

#### **C.5.3.5 SUBTASK 5 – ARCHITECTURE SUPPORT SERVICES**

USACE OCIO/G-6 requires infrastructure architecture support services to align USACE enterprise capabilities to the vision and direction of the overall USACE Enterprise Architecture (EA) effort. This shall ensure that USACE OCIO/G-6 service delivery can effectively support the current and future IT requirements of USACE end users and clients.

EA is systematically derived and captured descriptions depicted in models, diagrams, and narratives specifically using the current DoD Architecture Framework (DoDAF) views that shall be developed in industry standard tools (USACE currently support MagicDraw tool) and in technical terms (such as hardware, software, data, communications, security attributes, and performance standards). It provides these perspectives for the enterprise's current environment and for its target environment, and it provides a transition plan for moving from the current to the target environment. The contractor shall:

- a. Adhere to Engineering Regulation (ER) 25-1-112 Information Technology Architecture or successor documents.
- b. Develop, maintain, and update technical documentation describing the current EA and changes to Technical Baselines and Integrated Architecture Products (**Section F,**

**Deliverable 25)** for EA modifications in design/planning phase and/or post-implementation.

- c. Perform annual configuration audits to validate configuration items are accurately represented in the USACE Technical Baselines, Integrated Architecture Products, and design and installation documentation (**Section F, Deliverable 26**).
- d. Identify and keep a current comprehensive list of USACE data structures, sources, categorizations, and formats.
- e. Create or update design documentation to support all changes, new services, and technology refresh installations (**Section F, Deliverable 27**).
- f. Propose, design, and document location modifications to connect MAN or LAN to local Service Delivery Point (SDP) in accordance with location WAN circuit mapping.
- g. Deliver all design hardware and software specifications and Bill of Materials (BOM), including incorporation of input from the Government (**Section F, Deliverable 28**).
- h. Assess, validate, and update the mapping to USACE OCIO/G-6 systems in the USACE OCIO/G-6 product baseline. The update shall include the delineation of segment services.
- i. Provide as-built and network topology drawings (**Section F, Deliverable 29**):

#### **C.5.3.6 SUBTASK 6 – ENGINEERING DESIGN SUPPORT SERVICES**

The contractor shall provide Engineering Design Support Services (EDSS) that encompass the engineering and technical support services required to design, model, test, pilot, and implement the systems and infrastructure required to deliver IT projects including, but not limited to, voice, video, and data services, at the enterprise and local site levels. EDSS shall provide the Government with advice, assistance, investigation, coordination, and implementation services for improvement or addition to existing solutions or implementation of emerging solutions. EDSS shall incorporate cybersecurity requirements to ensure developed systems meet all cybersecurity requirements

#### **C.5.3.7 SUBTASK 7 – SOFTWARE DEVELOPMENT SERVICES**

The contractor shall establish a software engineering capability, available only when requested, that rapidly delivers secure and working products and software solutions. All source code developed and utilized by the contractor in performance of this subtask shall be provided to the Government, (**Section F, Deliverable 30**). The contractor's software engineering capability shall apply all relevant fields of engineering to include physical systems, requirements, design, development, testing, deployment, maintenance, and modernization of software systems.

The contractor shall establish software development lifecycle and engineering processes based on commercial best practices. In implementing this process, the contractor shall establish a DevSecOps pipeline that builds in security and maximizes the concept of Continuous Integration (CI)/Continuous Delivery (CD) that automates build, integration, and test processes. The software engineering capability shall enable an iterative approach to design, development, testing, and implementation. The contractor shall provide software registration portals to track



owner, developer, and requirements of produced software. The contractor shall provide results from software testing and requests needed for application whitelisting.

#### **C.5.3.8 SUBTASK 8 – ASSET AND CONFIGURATION MANAGEMENT**

The contractor shall provide asset management in accordance with ITIL best practices and DoD, Army, and USACE guidance. The contractor shall provide an Asset Management Plan (**Section F, Deliverable 31**). The contractor's Asset Management Plan shall include a complete solution to document and track USACE OCIO/G-6's hardware and software assets. The contractor shall perform lifecycle management, including reporting and maintaining version currency, vendor/manufacturer maintenance, property receipt, refresh, inventory control, equipment staging and distribution, warranty repair coordination, erasure and cleansing, and transfer or destruction of hardware assets.

The contractor shall provide configuration management based on ITIL, USACE and industry best practices. The configuration management solution (**Section F, Deliverable 32**) shall be capable of capturing and maintaining the varying attributes and relationships of the Configuration Items (CIs) necessary for IT service delivery and modeling proposed changes for impact analysis. The Configuration Management Database (CMDB) for OCIO/G-6 is the tool and database used to manage and model configuration data for OCIO/G-6 infrastructure assets from design to retirement. The CMDB tool collects, stores, manages, updates, and presents data about all CIs, including the relationships between CIs and services.

#### **C.5.3.9 SUBTASK 9 – SOFTWARE LICENSE AND HARDWARE MAINTENANCE AGREEMENT MANAGEMENT**

In coordination with USACE OCIO/G-6, the contractor shall develop and provide License and Agreement Management and Tracking Procedures (**Section F, Deliverable 33**) for each USACE CIO G/6 software license and/or maintenance agreement. When directed by the Government, the contractor shall purchase license and maintenance agreements for use by the USACE OCIO/G-6 users. The contractor shall ensure licenses and agreements are purchased in accordance with current OMB, DoD, and USACE policies. The contractor shall ensure that all software license transfers (e.g., the transfer of licenses during a device refresh and/or the transfer of licenses during resource attrition) are reflected in the applicable asset management system. Additionally, the contractor shall maintain the USACE OCIO/G-6 software library. The contractor shall maintain the USACE OCIO/G-6's centralized software library to ensure that media exists for each software asset; proof of entitlement and software restrictions or usage rights exists for each software asset; proof of maintenance exists for each software asset; media installation or other security codes to install software assets exists for each software asset; and all records and media are duplicated in an offsite location for DR purposes. The contractor shall develop and implement a process for individual users to request software, evaluate the request, provide recommendations for acceptance, and purchase and deploy software. Additionally, the contractor shall identify, document, and report license compliance issues by end users and recommend solutions to resolve issues. The contractor shall provide software license usage identifying additional licenses when appropriate and also making recommendations for removal. As USACE

OCIO/G-6 continues its migration to a Software-as-a-Service model (SaaS), the contractor shall provide support, including the management of enterprise licensing, identification of possible SaaS offerings that will benefit USACE, and implementation of SaaS solutions.

#### **C.5.3.10 SUBTASK 10 – SHAREPOINT DEVELOPMENT AND ADMINISTRATION**

The contractor shall provide SharePoint development and administration support to all USACE OCIO/G-6-supported organizations utilizing SharePoint sites.

#### **C.5.4 TASK 4 – CYBERSECURITY**

USACE, as an Organizational Network (ORGNET) Cyber Security Services Provider (CSSP) aligned under Army Cyber Command (ARCYBER), executes the cybersecurity activities and functions to direct the security, operations, and defense of the USACE-controlled portion of the Defense of Defense Information Network (DoDIN), consistent with all orders, regulations, policies, memorandums and/or directives to counter cyberspace threats and mitigate vulnerabilities. USACE OCIO/G-6 Cyber Security conducts the cybersecurity functions of identify, protect, detect, respond and recover within the CorpsNet infrastructure, USACE Enterprise SIPRNet, cloud environments owned or operated on behalf of USACE, CorpsNet connected SCADA and OT systems connected to CorpsNet, and the USACE agency-level instances of Joint Regional Security Stack (JRSS). USACE cybersecurity activities and functions ensure the availability, integrity, and confidentiality of the information and information systems used by USACE commands and mission areas. USACE OCIO/G-6 Defensive Cyber Operations (DCO) provides services for the protection, monitoring, analysis, detection, and response to unauthorized activity. DCO services are required to defend against unauthorized activity on all supported networks, to include, but not limited to, activities from advanced persistent threat actors, external hackers, insider threats, and all others who may attempt to gain unauthorized access.

The contractor shall provide cybersecurity services for USACE in accordance with all Federal, DoD, Army, and USACE-specific security initiatives. The contractor's cybersecurity services shall be proactive, continuous, and result in "inspection ready" systems and environments at all times, and shall be postured to achieve passing scores on all inspections, to include, but not limited to, no notice Command Cyber Readiness Inspections (CCRIs). The contractor shall implement all phases and aspects of DoD accreditation/certification policies and procedures for the USACE-controlled portion of the DoDIN during the entire lifecycle for all USACE systems and environments. The contractor shall provide consistent and complete documentation that satisfies all policy and reporting requirements TO ESTABLISH the USACE Reporting and Analysis Program, which reports to appropriate Federal, DoD, Army, and USACE organizational entities, such as the OMB, DoD Inspector General, DISA, Army Network Enterprise Technology Command (NETCOM), ARCYBER, Army CIO/G-6, and USACE OCIO/G-6 and Command staff.

The contractor shall develop a Cybersecurity Strategy Plan (CSP) (**Section F, Deliverable 34**), that describes concisely how a program's cybersecurity features comply with applicable

standards, regulations, and requirements. The CSP shall identify how the contractor shall meet the following subtasks.

#### **C.5.4.1 SUBTASK 1 – PATCHING AND VULNERABILITY MANAGEMENT**

The contractor shall implement, configure, operate, and maintain an automated patch and vulnerability management capability to maintain compliance for assets and technologies within the USACE controlled portion of the DODIN. In support of patching and vulnerability management, the Contractor shall:

- a. Maintain current anti-malware, software, engines, and signatures, vendor patches, IAVM, in accordance with DoD, Army, and USACE OCIO/G-6 directives, policies, and procedures
- b. Minimize the impact of patching and scanning on USACE operations and end users.
- c. Maintain proactive awareness of changes in the threat landscape and/or vulnerabilities and propose and execute mediatory actions.
- d. Implement a process for emergency vulnerability notifications for accelerated timelines.
- e. Comply with DoD, Army, and USACE OCIO/G-6 reporting requirements.
- f. Conduct and analyze STIG, IAVM, and non-IAVM scans. Address and mitigate non-compliant devices or configurations, adhering to the organizational change management process (**Section F, Deliverable 35**).
- g. Conduct vulnerability tests within a test environment to identify operational impact of activity directed against USACE systems or applications to identify USACE-wide impacts as requested.
- h. Provide a Plan of Actions and Milestones (POA&M), Operational Impact Statements (OIS), or Waiver if STIG(s) or IAVMs cannot be achieved, providing mitigation/remediation strategies to reduce risk to achieve STIG compliance (**Section F, Deliverable 36**).
- i. Schedule, assign, and monitor POA&M action items until completion by or before the established suspense date.
- j. Report status of STIGs or IAVMs for all applicable technologies, assets, etc. (**Section F, Deliverable 37**).
- k. Ensure no un-remediated AVMs exist on the network without an approved POA&M or Waiver or one that has been preceded with a later IAVM version.
- l. Ensure correlation of STIG and IAVM-required audit and accountability transaction alerts are fed into Security Information and Event Management (SIEM).

#### **C.5.4.2 SUBTASK 2 – STRATEGY, POLICY, AND CONTINUOUS IMPROVEMENT**

The contractor shall analyze the current USACE OCIO/G-6 security strategy, posture, policies, and operations to identify areas for improvement (**Section F, Deliverable 38**). Improvements may be based on best practices or new technologies and shall be appropriate for all environments and missions. The contractor shall support continuous improvement and shall:

## SECTION C – PERFORMANCE WORK STATEMENT

- a. Review, assess, and recommend mitigation actions on new vulnerabilities (e.g., zero-day etc.).
- b. Enhance performance of asset data collection and maintenance.
- c. Collect and analyze lessons learned for potential process improvements and incorporate applicable lessons learned into current policies, guidelines, checklists, procedures, and/or other appropriate means. All lessons learned shall be documented and maintained in the contractor's TO portal.
- d. Provide budget and fiscal support which includes, but is not limited to, analysis and documentation of budgetary information as it relates to meeting requirements, risk discussion, return on investment, value, and outcome.

### **C.5.4.3 SUBTASK 3 – MANAGED SECURITY SERVICES (MSS)**

USACE OCIO/G-6 requires MSS to safeguard USACE-supported networks and systems against ever-evolving security threats. MSS provide protection of endpoints, email, web, and networks, and include capabilities such as authentication, antivirus, anti-malware/spyware, intrusion detection, and incident response. The contractor shall provide up-to-date situational awareness of network security services, devices, and resources associated with MSS, including, but not limited to, Application Filtering (Layer 7), Network Time Protocol (NTP), Domain Name Service (DNS) protocol including Domain Name System Security Extensions (DNSSEC), external registration and management, malware domain prevention/detection, malware inspection and prevention, behavior-based intrusion detection and analysis, rogue wireless access point detection and prevention, deep packet inspection and analysis, source and destination address filters, including automated Access Control List (ACL) review and policy compliance, Transmission Control Protocol (TCP) stream data capture with access to archival information for forensics purposes, Reverse Web Proxy (RWP), and secure channel inspection, analysis, and prevention.

MSS is further broken out into:

- a. Monitoring services
- b. Vulnerability Scanning Services (VSS)
- c. Incident response services (INRS)

While identified here as separate activities, the contractor shall provide services in a holistic manner, with each individual service supporting and reinforcing the other to provide a complete MSS.

Monitoring services provides the ability to monitor hosts and network traffic, and analyze network protocol and application activity to identify and mitigate suspicious activity. This service will be provided 24/7/365.

VSS searches for security weaknesses, flaws, and open exploit vectors on the USACE OCIO/G-6 systems, networks, and applications. VSS can also simulate a real intrusion in a controlled environment, to gauge a network's susceptibility to attacks. This service will be provided 24/7/365. The service performs controlled internal and external scanning by remotely probing a

## SECTION C –PERFORMANCE WORK STATEMENT

network for penetration weaknesses that generally come from the outside, and internal scans that detect flaws originating from the inside.

INRS, in accordance with the Chairman of the Joint Chief of Staff Manual (CJCSM) 6510.01B Cyber Incident Handling Program, involves telephone, web, and on-site support for monitoring and analyzing alert information, and responding to malicious events such as Denial of Services (DOS) attacks; virus, worm, and Trojan horse infections; and illegal inside activities, espionage, and compromise of sensitive internal agency databases. This service shall be provided 24/7/365. INRS shall provide support through all phases of incident response (preparation, identification, containment, eradication, and remediation). INRS shall provide an effective method of addressing these security intrusions, thereby ensuring operational continuity in case of attacks.

MSS shall connect to and interoperate with the agency networking environments, including cloud, DMZs and secure LANs, as required by the USACE OCIO/G-6. The service shall also support connectivity to extranets and the internet.

Monitoring services shall include, but are not limited to:

- a. Providing analysis and monitoring for all systems and environments to ensure the availability, integrity, and confidentiality of the data processed, stored, and transmitted via a centralized support monitoring service. Analysis and monitoring shall be automated to the maximum extent possible.
- b. Providing Intrusion Detection System/Intrusion Prevention System (IDS/IPS) support:
  - i. Implementing, administering, and maintaining threat sensors based on current threat directives and recommendations.
  - ii. Developing, testing, and distributing threat sensor baseline signatures.
  - iii. Developing IDS/IPS test plans, operational procedures, and maintenance plans **(Section F, Deliverable 39)**.
  - iv. Providing host-based intrusion detection monitoring and prevention on all devices, including those supporting Host-Based Security Systems (HBSSs).
  - v. Providing data feeds from all intrusion detection and prevention modules for incorporation into the Enterprise Security Incident Management System, for CorpsNet, cloud, DMZ, and SIPR in accordance with classification guidance.
- c. Providing continuous monitoring of malware protection and detection mechanisms.
- d. Providing administrator access to the designated Government POCs as required.
- e. Providing active monitoring of the operational status, health, and performance of the monitoring tools and devices.
- f. Actively monitoring vendor feeds, Army feeds, tippers, OPORDS, sensor grids, and intelligence feeds for new signature information.
- g. Analyzing the information provided and providing recommendations for inclusion into the CorpsNet, and SIPRNet environments, while maintaining the classification of information.
- h. Providing performance measurements, logs, and information feeds from the security monitoring systems (e.g., HBSS and IPS).

## SECTION C –PERFORMANCE WORK STATEMENT

- i. Maintaining access to current network architecture diagrams per DISA standards showing placement of sensors (e.g., IDS/IPS, Routers, Netflow/PCAP systems, firewall, etc.).
- j. Reporting on access to assets, including, but not limited to, network and host-based sensors for CorpsNet, CorpsNet extended network (JRSS and cloud), and SIPRNet (**Section F, Deliverable 40**).
- k. Integrating and correlating data from USACE systems, servers, services, SIEM, and end points to measure, monitor, remediate, and remove threats to the environment in accordance with USACE OCIO/G-6 directives.

VSS shall include, but are not limited to:

- a. Performing monthly wireless scanning to monitor for non-approved or rogue wireless access points.
- b. Developing and maintaining scan zones for out of compliance conditions based on USACE OCIO/G-6 directives. As required, conduct ad hoc scans. Scans can be full system, specific workstation, or server scans. The contractor shall analyze scan results and provide a Recommendations Report (**Section F, Deliverable 41**).
- c. Providing vulnerability testing in accordance with DoD, Army, and USACE OCIO/G-6 directives and guidance and established best business practice regulations, policies, and procedures.
- d. Identifying existing defensive weaknesses or vulnerabilities. Providing assessment to USACE OCIO/G-6 to determine the best method of mitigation or continued monitoring (**Section F, Deliverable 42**).

INRS shall include, but are not limited to:

- a. Responding to alerts and violations identified, in accordance with cyber policy and incident response plans, as part of the SIEM.
- b. Identifying incident threat level and nature based on the received alert or violation.
- c. Identifying root cause, source, and methodology used to properly categorize the incident.
- d. Providing AR 380-53 Network Damage Assessment, if necessary.
- e. Gathering host logs from compromised system(s).
- f. Taking corrective action to contain the incident, prevent further spread, and protect systems.
- g. Providing forensically sound evidence collection and capabilities.
- h. Eradicating the malicious event from infected hosts/network as directed by USACE OCIO/G-6.
- i. Providing cyber clean-up as required, including the restoration of damaged data.
- j. Recommending mitigating actions to prevent future infections or reinfection.
- k. Configuring and fine-tuning detection/prevention capabilities.
- l. Providing cyber After Action Reports (AARs), including lessons learned and final network damage assessment as identified by USACE OCIO/G-6 (**Section F, Deliverable 43**).

## SECTION C – PERFORMANCE WORK STATEMENT

- m. Providing analysis, correlation, and trending of anomalous events and incidents.
- n. Supporting incident response team deployment to USACE OCIO/G-6 locations.
- o. Coordinating and sharing data with other Federal agencies and DoD commands as directed by USACE OCIO/G-6.
- p. Providing analysis and reverse engineering of cyber threats.
- q. Implementing mitigation measures in response to general or specific threats on the respective networks in accordance with USACE OCIO/G-6 directives.

### **C.5.4.4 SUBTASK 4 – SECURITY INFORMATION AND EVENT MANAGEMENT SUPPORT**

The contractor shall implement, configure, monitor and maintain a DoD-approved enterprise SIEM tool to monitor, detect, and respond to threats on all USACE-supported networks and enclaves. The SIEM shall provide real-time analysis of security alerts generated by applications and network sensors, hardware, cyber tools, Government-approved threat intelligence feeds and threat detectors, and be capable of automatically forwarding incidents and events to the incident response team and USACE OCIO/G-6 based on severity level. The SIEM shall be configured to support classification level of data. Additional support for the SIEM shall include, but is not limited to:

- a. Automated incident response capabilities.
- b. Performing data correlation and analysis reporting for all sensors and defense capabilities at an enterprise level.
- c. Providing the Government access to the SIEM systems, including the functionality to establish use cases and run queries.
- d. Providing immediate notification for unplanned sensor-fed outages exceeding 24 hours, and providing an AAR identifying root causes for the outage (**Section F, Deliverable 44**).
- e. Maintaining documentation for all feeds, sensors, and connectors in the SIEM and providing reports to USACE OCIO/G-6 (**Section F, Deliverable 45**).

### **C.5.4.5 SUBTASK 5 – CONTINUITY OF OPERATIONS (COOP) AND DISASTER RECOVERY (DR) SERVICES**

The contractor shall provide IT support to USACE OCIO/G-6 COOP and DR efforts and site(s). The contractor shall develop and execute a COOP/DR Plan (**Section F, Deliverable 46**), as directed by the Government, for USACE OCIO/G-6 COOP and DR capabilities. This plan will be exercised periodically to ensure that safeguards, backups, end-user services, and procedures can provide continuity of mission support services through issues such as natural disasters, power outages, and building loss, and allow for successful recovery of all services after facility restoration or the establishment of an alternate facility.

The contractor shall provide the following COOP-related services as directed by the Government:



## SECTION C –PERFORMANCE WORK STATEMENT

- a. Provide IT-related technical input to USACE OCIO/G-6 COOP planning, design, and implementation efforts, including meeting and briefing support.
- b. Provide IT-related technical liaison, coordination, and Tier I/II support with COOP facility service providers.
- c. Ensure USACE OCIO/G-6 systems remain viable in the event of system failover.
- d. Perform scheduled COOP exercises to ensure functional and operational processes are current to infrastructure changes and are held annually at a minimum.

The contractor shall provide the following DR-related services as directed by the Government:

- a. Provide technical support to DR meetings.
- b. Support technical assessment and perform site surveys for DR candidate sites and hosting services in support of Government planning activities.
- c. Assist USACE OCIO/G-6 in developing and documenting DR capabilities.
- d. Support and administer network connectivity, cryptography, circuits, and other communications systems between USACE OCIO/G-6 and DR facilities.
- e. Provide IT-related technical support to the operation of USACE OCIO/G-6 DR capabilities.
- f. Support implementation, configuration, and administration of DR systems
- g. Perform scheduled DR exercise to ensure the DR Plan and documentation remains up to date and current.

### **C.5.4.6 SUBTASK 6 – CYBER TOOLS SUPPORT**

The contractor shall propose, develop, install, manage, maintain, integrate and configure a suite of cybersecurity tools to support USACE CIO G-6 network cybersecurity posture. Cybersecurity tools include, but are not limited to, hardware and software throughout CorpsNet, CorpsNet Extended Networks (CEN), network exit points, and endpoint devices performing detection, protection, prevention, analysis, response, and remediation of cyber security threats. Support shall include, but not be limited to:

- a. Developing software enhancements for cyber tools and re-utilization of code, in accordance with USACE CIO G/6 priorities.
- b. Developing supporting documents and maintenance schedules (**Section F, Deliverable 47**).
- c. Ensuring repositories for cyber tool backups, cyber tool configurations, scan repositories, and analysis portals are created, maintained, and available.
- d. Testing and verifying for reliability backups, configuration changes, and updates.
- e. Providing analysis of all monitoring tools, including, but not limited to, audit logs, IDS/IPS logs, firewall logs, audit logs, access logs, and full packet capture data for covert or malicious activity.



#### **C.5.4.7 SUBTASK 7 – THREAT INTELLIGENCE SERVICES**

The contractor shall provide cybersecurity intelligence support to identify emerging threats to the USACE OCIO/G-6 environment. The contractor shall provide the following support:

- a. Develop and report tailored, all-source analysis to provide situational awareness of critical elements of the cyber environment necessary to defend the USACE and USACE extended networks (**Section F, Deliverable 48**).
- b. Maintain awareness of current activity trends on Army, other Government, and commercial networks.
- c. Contribute to the body of knowledge on bad actors or adversaries' cyber capabilities and intentions.
- d. Develop a priority list of high-profile personnel and groups to track. This list should include all named activities as well as other people/groups of interest.
- e. Analyze the origins, pathways, and methodologies of malicious cyber activities to attribute, model, and predict future intrusions.
- f. Analyze computer network intrusion events and malicious activity to support intrusion detection and cyber-attack warning and response.
- g. Provide forensic analysis of captured packets, hard drive images, system logs, and sensor data used in all-source intelligence products.
- h. Perform Requirements Management (RM) to track intelligence requirements and production efforts. Maintain record of all relevant cyberspace operations reports and task assignments for tracking purposes.
- i. Update, maintain, and ensure quality control of appropriate classified databases and repositories.
- j. Maintain liaisons and conduct technical exchanges with parent agencies and vetted partners' higher agencies. Identify exchange opportunities and conduct exchanges (formal and informal) as appropriate.

#### **C.5.4.8 SUBTASK 8 – SECURITY CONFIGURATION MANAGEMENT (SCM)**

SCM provides an enterprise-wide security compliance capability , 24/7/365, that scans and remediates USACE OCIO/G-6 IT assets, services, and all end points for out of compliance conditions such as changed settings, outdated patches, and un-approved software IAW CJCSM 6510.01B and DoD, Army, and USACE directives, policies, and procedures. The contractor shall collaborate with the Government and other service providers to provide the services. In support of SCM, the contractor shall provide the following, including, but not limited to:

- a. Providing central administration of overall USACE OCIO/G-6-related network SCM status, in combination with the Government.
- b. Providing SCM scanning, data collection, and analysis.
- c. Remediating and mitigating assigned SCM configurations in accordance with USACE OCIO/G-6 response processes.
- d. Executing end-to-end data correlation.

## SECTION C –PERFORMANCE WORK STATEMENT

- e. Documenting configuration parameters.
- f. Maintaining the current SCM tools and databases.
- g. Identifying compliance capability gaps and recommending SCM tool optimizations to enhance performance and/or reduce user impact.
- h. Reporting the availability, capacity, and performance of the security infrastructure and services.
- i. Supporting authorized third-party evaluators performing vulnerability evaluations.
- j. Updating SCM tools and database signature files as required.
- k. Managing, maintaining, and documenting the configuration and operability of the cyber tools, databases, and logs.
- l. Maintaining security configuration of cyber network defense devices.
- m. Providing quarterly analysis of SCM transport services, systems, and networks to identify potential security weaknesses and exposures to known threats.
- n. Providing Enterprise DAT Versioning and enterprise virus scanning software versioning reporting as required (**Section F, Deliverable 49**).

### **C.5.4.9 SUBTASK 9 – DEMILITARIZED ZONE (DMZ) SERVICES**

A DMZ is a logical and physical framework that allows protected access to resources from internal and external networks. Extended-DMZ (e-DMZ) or DMZ extension is a combination of hardware and software that creates a logical addition from a different physical facility to 1) the DMZ resources; or 2) a single zone in the e-DMZ.

The contractor shall:

- a. Implement and maintain the DMZ infrastructure in accordance with applicable directives, policies, and OPORDs.
- b. Provide DMZ configuration documentation and store appropriately.
- c. Apply applicable cybersecurity and cyber change management policies when requesting and making changes.
- d. Provide biannual verification and analysis of DMZ configurations and any recommendations for improvement.
- e. Maintain a Bogon list and ensure implementation of Bogon updates and filters is performed within 24 hours, unless emergency conditions require a more immediate deployment..
- f. Verify and monitor enforcement of public-facing web server security configurations, RWP, web content and filtering policy, and firewall action requests. Perform an annual review and analysis of each public web server, RWP policies, and Web Content Filter (WCF) rules. Generate an annual report that reviews, analyzes, and provides recommendations for each of the DMZ web servers, RWP, and WCF. (**Section F, Deliverable 50**)
- g. Review new web deployments, policies, and rules; document findings and create actions to correct security issues; and provide notification to proper organizations for follow up.

**C.5.4.10 SUBTASK 10 – PENETRATION TESTING (PEN-TESTING)**

USACE's cyber security program is periodically required to provide results of penetration testing (pen-testing) of USACE networks and systems to validate the success of implemented security controls. The contractor shall support pen-testing of USACE networks in coordination with the Government. The contractor shall:

- a. Support pre-pen testing efforts:
  - 1. Provide device and system availability for testing.
  - 2. Provide network drawings/design documentation in accordance with classification requirements and policies.
  - 3. Provide internal and external network configurations required to perform pen-testing.
- b. Support pen-testing activities:
  - 1. Escort pen-test and Red Team personnel during on-site activities.
  - 2. Support pen-test exercises as directed by the Government.
  - 3. Provide a liaison between on-site pen-test and Red Team and Government personnel, documenting activities, findings, incidents, and weaknesses.
- c. Support post-pen testing and Red Team efforts:
  - 1. Provide analysis of pen-testing results, including a summary of security weaknesses, risks to CorpsNet and SIPRNet, and recommendations to secure the weaknesses identified (**Section F, Deliverable 51**).
  - 2. Implement approved security recommendation in accordance with USACE OCIO/G-6 directives.

**C.5.4.11 SUBTASK 11 – PORTS, PROTOCOLS AND SERVICES MANAGEMENT (PPSM)**

The Ports, Protocols, and Services Management (PPSM) program requires USACE OCIO/G-6 under DISA, to register and carefully manage all DoD Information Systems and whitelist registrations, including the use of network Ports, Protocols, and Services (PPS). USACE OCIO/G-6 utilizes DISA's Category Assurance List (CAL) when preparing USACE projects for development and acquisition. The contractor shall support the PPSM program by:

- a. Ensuring that all DoD information systems PPS that are accessible to the managed networks are acquired, developed, implemented, and registered in the PPSM central registry.
- b. Using and protecting PPS according to the most current vulnerability assessment reports, and implementing them as described in the most current version of DoD STIGs on network infrastructure and application security and development.
- c. Implementing and enforcing PPSM policies and procedures at the enclave boundaries, and restricting boundary firewalls and firewall-like devices to the use of approved PPS in accordance with DoDI 8551.01 or successor documents.
- d. Reviewing software, hardware, and PPS against the Approved Products List, evaluated product list, and DISA CAL.

## SECTION C – PERFORMANCE WORK STATEMENT

- e. Conducting auditing, in accordance with the approved test plan, to verify that the designated site complies with DoD, Army, and USACE OCIO/G-6 policy.
- f. Performing blocking/denying access by hostile sites or restricting access by specific ports/protocols and/or applications in accordance with USACE OCIO/G-6 policies.
- g. Coordinating with DoDIN, DISA, and Army network staff as required for network configuration modifications (e.g., IP blocks/un-blocks and Uniform Resource Locator (URL)/domain blocking/unblocking) in accordance with cyber change management processes.
- h. Providing PPSM management in support of changes to network and service requirements (e.g., workload migrations to cloud hosting, etc.).

### **C.5.4.12 SUBTASK 12 – RISK MANAGEMENT FRAMEWORK (RMF) SUPPORT**

The contractor shall provide cybersecurity authorization and compliance services supporting the RMF for USACE in accordance with DoD, Army, and USACE OCIO/G-6 policies and procedures.

The contractor shall provide technical support in collaboration with USACE cybersecurity groups and technical teams to provide RMF support through the six steps of the RMF process. The contractor shall support USACE in the development of security plans, generation of assessment reports, and formulation of a remediation POA&M. The contractor shall perform the following tasks:

- a. Categorize agency information systems
- b. Select security controls
- c. Implement security controls
  - 1. Produce and provide security control artifacts required by DISA for interim authority to connect and authority to connect (**Section F, Deliverable 52**).
- d. Assess security controls:
- e. Authorize information systems and provide Information System Security Manager (ISSM) services
- f. Monitor security state
  - 1. Capture, assess, maintain, and report asset information and provide an assessment report, identifying issues related to capturing of data and/or storage of data (**Section F, Deliverable 53**).

### **C.5.4.13 SUBTASK 13 – FILE REMOVAL SERVICES**

File removal services provide isolation and resolution when electronic spillage has occurred where classified or controlled unclassified (such as Personally Identifiable Information (PII)) information has been introduced on an IT system, network, or component that is not authorized to hold or process such information. A spillage can be from a higher level classification to a lower one. The data itself may be residual (hidden) data or metadata.

The contractor shall provide support for both classified and PII spillage

## SECTION C –PERFORMANCE WORK STATEMENT

- a. For classified spillage:
  1. Notify the activity in accordance with DoD, Army, or USACE OCIO/G-6 policies when there are incidents involving possible or actual compromise or data spills of classified information resident in information systems, as required.
  2. Quarantine known electronic spillage locations in accordance with cyber security directives and USACE policies.
  3. Remove all instances of the electronic spillage from the network, back-up systems, email, mobile devices, printers, and media in accordance with cyber security directives and USACE policies. Spillage locations that cannot be electronically removed shall be coordinated with designated personnel to remove and verify the electronic spillage.
  4. Start the trace process to determine the extent of the electronic spillage proliferation across systems.
  5. Provide spillage reporting as required, including, but not limited to, trace reporting, the last known locations of files that may have been further distributed but cannot be traced to service-level NOCs, and unauthorized or inadvertent disclosure summary data and results (**Section F, Deliverable 54**).
  6. Submit a POA&M for actions that cannot be completed within timeframes required by USACE policy (**Section F, Deliverable 55**).
  7. Notify the designated Government authority upon completion of electronic spillage cleanup.
- b. For PII spillage
  1. Follow incident reporting procedure as outlined in USACE-IT PII SOP upon notification of a PII breach by the customer.
  2. Report PII to the U.S. Computer Emergency Readiness Team (US-CERT) and immediately upon notification of an incident; annotate the helpdesk ticket with the US-CERT incident number.
  3. Send PII notifications to the USACE Privacy Officer as well as to other distribution groups as defined in the USACE-IT PII SOP.

### **C.5.4.14 SUBTASK 14 – CYBER FORENSICS AND MALWARE ANALYSIS (CF&MA)**

The CF&MA mission supports the USACE in the areas of file data collection, volatile data collection, analysis of system anomalies, malware reverse engineering, and creation of Indicators of Compromise (IOC) to improve the protection of USACE information. The USACE CF&MA works in concert with the Army Cyberspace Operations and Integration Center (ACOIC) and ARCYBER to ensure electronic evidence collection and integrity are maintained throughout the lifecycle of the evidence.

The contractor shall:

## SECTION C – PERFORMANCE WORK STATEMENT

- a. Perform forensically sound electronic data collections, analysis and reverse engineering of malware, suspect code, email, malformed program objects, and volatile memory in accordance with USACE OCIO/G-6 directives, and chain of custody guides utilizing industry best practices.
- b. Analyze the attack/exploit capability of malware as directed by USACE OCIO/G-6.
- c. Provide all pertinent findings and IOCs to teams responsible for the development of signatures to detect the malware as it propagates on infected systems.
- d. Collect, preserve, and transfer forensic evidence of unauthorized access to CorpsNet devices or information systems in accordance with USACE OCIO/G-6 policy and processes.
- e. Produce analysis reports for each incident and provide them to USACE OCIO/G-6.
- f. Work and interact with professionals, internal and external to USACE, to understand higher-level adversary capability.
- g. Document, update, and enhance processes and procedures by producing training materials, tools, tactics, techniques, procedures, SOPs, lessons learned, and reports.

### **C.5.4.15 SUBTASK 15 – CYBER PLANS AND EXERCISE SUPPORT**

The contractor shall support USACE OCIO/G-6 cyber plans and exercises to assess, evaluate, and update the USACE OCIO/G-6 cyber posture.

- a. Administer the development, planning, and exercises to be performed.
- b. Attend exercise planning conferences, provide expert advice for development of planning documentation, participate during exercise and other security cooperation events, and prepare AARs and lessons learned during all phases of DCO support exercises.
- c. Support mission planning, mission analysis, technical analysis, and Concept of Operations (CONOPs).
- d. Develop and/or provide input to OPORDs, CONOPs, and courses of action.
- e. Support management and planning operations by submitting mission requests, providing status reports, and submitting AAR comments

### **C.5.4.16 SUBTASK 16 – INSPECTION AND AUDIT SUPPORT**

USACE OCIO/G-6-supported environments are subjected to a variety of inspections, audits, and external reviews, including, but not limited to, the Command Cyber Readiness Inspection (CCRI), FISMA, TMF, Security Control Assessor-Validator (SCA-V), Army Protection Program Assessment (APPA), DoD Inspector General (IG), Chief Financial Officer (CFO) audits, and CSSP reviews. The contractor shall strive to conduct all cybersecurity support to provide an always audit-ready solution. The contractor shall:

- a. Ensure notification and tracking of significant incidents that meet CCRI criteria.
- b. Prepare and maintain network address declarations in accordance with DISA requirements. Changes shall be submitted to the USACE OCIO/G-6 for approval.

## SECTION C – PERFORMANCE WORK STATEMENT

- c. Provide support for inspections, audits, and external reviews, including pre- and post-audit support.
- d. Provide audit readiness assessments. Assessments include, but are not limited to:
  - 1. Review of documentation for accuracy.
  - 2. Provide status of STIG, vulnerability, misconfigurations, etc.
  - 3. Provide Category (CAT) I, II or III remediation statistics.
  - 4. Estimate CCRI Scoring based on JFHQ-DoDIN CCRI Scoring, CCRI Phase IV Grading Criteria Worksheet, and CCRI Risk Indicator Scoring.
  - 5. Identify key issues affecting the defense of the USACE networks and cyber posture.
- e. Identify systemic causes of any assessment finding, pre-audit and post-audit, and develop recommended courses of corrective actions.
- f. Develop and disseminate mitigation/remediation guidance throughout the organization.
- g. Ensure participation in any meetings, to include travel for any assessment, pre-audit, audit, and post-audit.

### **C.5.4.17 SUBTASK 17 – OPERATIONAL ORDERS (OPORDS) AND TASKINGS**

The contractor shall support USACE OCIO/G-6 OPORDS and taskings. The Contractor shall:

- a. Analyze and comply with assigned OPORDs/taskers within the assigned suspense date, making recommendations to service owners.
- b. Review, draft, and obtain technical input for OPORDs, Fragmentary Orders, TASKORDs, and other system-requirements documentation.
- c. Test and implement procedures to mitigate vulnerabilities or comply with other actions in the OPORD/tasker.
- d. Develop POA&M and OISs within timelines of individual orders.
- e. Track all assigned OPORDs/taskers and approved POA&Ms until completion and acceptance by the Government.

### **C.5.5 TASK 5 – TELECOMMUNICATIONS**

USACE requires ongoing, scalable telecommunications services. The contractor shall provide a full range of telecom voice and data enterprise wired and wireless connectivity and services that provide connectivity to each USACE identified site. During TO performance, the need to establish services at additional locations will occur, as well as the need to terminate services at various locations, and the TO TDL process identified in **Section H.15** shall apply. The contractor shall also provide secure, reliable transport of agency applications across a high-speed, unified, multi-service IP-enabled backbone infrastructure. The contractor shall develop and maintain a Telecommunications Management Plan (TMP) detailing the status of services (i.e. Circuits, Devices, Mobile, etc.) at each location and any planned updates or changes (**Section F, Deliverable 56**). USACE customers and end users at main offices, field sites, and vessels rely on this technology to accomplish mission tasks. Additionally, some users rely on remote wireless access, and the contractor shall support as required.

## SECTION C – PERFORMANCE WORK STATEMENT

For each telecommunications support area, the contractor shall:

- a. Continually monitor current commercially available service offerings and technology advancements, and make recommendations to USACE for implementation.
- b. Ensure all designs and implementations provide customers appropriate bandwidth, latency, interoperability, etc., that enables uninterrupted voice, video, and data technologies at any USACE location. Procure all necessary infrastructure components and service plans.
- c. Ensure designs and implementations are in accordance with DoD, Army, USACE, and industry standards and best practices where USACE standards do not currently exist.
- d. Coordinate service delivery with other services providers to ensure seamless service to USACE end users.

### **C.5.5.1 SUBTASK 1 – TELECOMMUNICATIONS EXPENSE MANAGEMENT (TEM)**

The contractor shall provide a total solution for expense management for the entire USACE wired, wireless, voice, and data environment to optimize the enterprise operating expenses. The contractor shall provide contract administration, inventory management, invoice management, audit services, call detail report services, rate plan optimization, advanced analysis and reporting, contract optimization, ordering and procurement services, dispute management and recovery, help desk, and transition services. The contractor shall make TEM information available through the contractor-provided portal. Expense information shall be available by district, site, office, function, and user level as appropriate to support analysis.

### **C.5.5.2 SUBTASK 2 – MOBILE COMMUNICATIONS SOLUTION**

The contractor shall develop, plan, and implement an efficient, effective, and comprehensive mobile communications solution that provides all USACE users (CONUS and OCONUS) access to the most effective current, Government-approved commercially available service offerings (network, device, or other technology). The mobile communications solution shall be scalable (devices and network capability) and enhance the ability of USACE end users to conduct business.

The contractor shall assume operation of the current Government owned MDM solution and after award the contractor is expected to propose and ultimately provide a Mobile Device Management (MDM) solution that encompasses complete service lifecycle. The MDM solution shall include the limited provisioning of mobile devices technical support, activation of mobile communications plans (voice and data) deactivation of mobile communications plans, and any requisite additions, moves, or changes, and the eventual refresh, replacement, and disposal of mobile devices. The MDM solution shall be capable of provisioning mobile devices and services provided by other separate USACE contract vehicles. When service and devices are not provided separately, the RITS provider shall coordinate directly with regional or local carriers to meet USACE requirements. The contractor shall ensure its solutions provide customers appropriate bandwidth, latency, and interoperability to carry out mission-related activities. The contractor's solution may provide a complex and comprehensive strategy utilizing the services of multiple



## SECTION C – PERFORMANCE WORK STATEMENT

vendors to optimize services in different locations to maintain effective service levels. However, at a minimum, service agreements shall be at the district level and also include international capability and compatibility.

The contractor's MDM solution shall provide integrated functionality with the USACE enterprise's applications to maximize end-user productivity and access. The end user/customer interface for the MDM solution shall be the IT service desk and contained in the contractor's portal solution. The contractor shall provide management-level information for enterprise mobile device usage and metrics.

### **C.5.5.3 SUBTASK 3 – AUDIO/WEB CONFERENCING AND CASTING SERVICES (AWCCS)**

USACE OCIO/G-6 requires reservation less AWCCS available to all USACE end users to meet, present, and interact with information via a web browser, thereby allowing end users to share audio, video, information, documents, or applications interactively via the internet and the agency's intranet for audiences ranging from 2 to 50,000 geographically distributed participants.. A method to ensure content protection and authenticate users shall be included. This service shall have the ability to record sessions. The contractor shall continually update and maintain these services to remain current with commercial technology.

### **C.5.5.4 SUBTASK 4 – NETWORK CONNECTIVITY SOLUTION**

The contractor shall develop, plan, acquire on behalf of USACE, install, and manage innovative, high-performance connectivity solutions for USACE networks. This includes various connection topologies, including wired and wireless (cellular, microwave, Satellite Communication (SATCOM)), reach-back at both common (district/division) and non-standard locations (hydroelectric stations, parks, locks, dams, etc.). Service connectivity can be delivered using various combinations of IP transport media. (e.g., copper, fiber, Wi-Fi, cable, cellular, satellite). Individual connections shall be consolidated at locations to be determined by the provider (meet-me type co-located facilities). These connection points shall require high speed/high bandwidth/low latency connections to the internet, alternate networks (DoDIN, SIPRs) and cloud providers, external telecom providers, and content delivery providers. This core infrastructure shall be designed as a multi-carrier environment with diverse multiple connections. Route/carrier diversity is envisioned to minimize impact from any nationwide and regional outages. Additionally, incorporating "last-mile," diverse on-site fiber entry is envisioned to minimize impact from any local fiber cuts or central office equipment failures. All contractor-provided connectivity solutions shall support analog- and IP-based voice services, and the contractor shall modernize existing connections to Ethernet-based (public or private) transport to increase service performance as required.

The combined core infrastructure and vendor-owned consolidation points (meet me co-location) shall provide worldwide access using technologies such as carrier-agnostic Software Defined Wide Area Network (SD-WAN), bandwidth on demand, remote access (VPN) software clients, and support of zero-trust environments.

## SECTION C – PERFORMANCE WORK STATEMENT

Government-provided services such as Iridium, DoDIN, SIPRNet, Broadband Global Area Network (BGAN), Inmarsat, Short Burst Data, DSN, very-small-aperture terminal (VSAT) Bandwidth, Joint Worldwide Intelligence Communications System (JWICS), etc., will be directly coordinated with the Government team for Designated Agency Representative (DAR)-related processing/actions.

### **C.5.6 TASK 6 – TRANSFORMATION**

The USACE OCIO/G-6 environment is a dynamic, ever-changing environment, supporting the USACE global mission. In response to an evolving landscape, and in support of the USACE OCIO/G-6 strategic goals and objectives, the contractor shall provide transformation support that includes development of business processes and enterprise IT solutions, including innovative and emergent technologies focused on meeting overall objectives.

The contractor shall provide a dedicated workforce tasked with innovative, continual business process improvements leveraging advancements in technology and best industry practices to support the missions of the USACE and deliver service improvement. Transformations may begin as the result of a Government-identified problem or requirement or as a contractor-presented solution to a USACE mission. Transformation is designed to ensure process improvement is consistent, deliberate, and predictable. The contractor shall develop and deliver proposed innovations to the Government via a USACE led Innovation Review Board for review and approval. Approved innovations will be submitted to the FEDSIM COR for approval prior to implementation (**Section F, Deliverable 57**).

#### **C.5.6.1 SUBTASK 1 - PROVIDE STRATEGIC PLANNING SERVICES**

The contractor shall provide recommendations on the design, development, implementation, and maturation of IT service management, not only as an organizational capability, but also as a strategic asset. The contractor shall provide recommendations on the principles underpinning the practice of IT service management to aid the development and modernization of USACE OCIO/G-6 service management policies, guidelines, and processes. The contractor shall assist the USACE OCIO/G-6 in translating IT strategic goals, commitments, and objectives into actionable plans, tasks, activities, technology, and/or process solutions and possible alternatives, including the estimated costs for the various options, and the potential risks associated with each alternative. The contractor shall develop and implement IT service management plans, practices, infrastructures, and systems utilizing industry best practices to optimize enterprise-wide IT service delivery and improve operational performance with minimal impact on the IT enterprise

### **C.5.7 TASK 7 – EMERGENCY RESPONSE**

USACE provides support to the FEMA and other Federal, state, local, and tribal entities during national and natural emergency response and recovery operations. USACE OCIO/G-6 emergency response services provide IT capabilities in support of operations other than war (e.g., disaster relief, defense support to civil authorities, and foreign humanitarian assistance). Such services are primarily in support of emergencies or contingency operation and also directly support the Enterprise Emergency Response Team. The Enterprise Emergency Response Team

## SECTION C –PERFORMANCE WORK STATEMENT

uses Fly-Away Kits (FAK) consisting of CorpsNet components that augment existing services to provide a mobile virtual CorpsNet environment for emergency or contingency response. A single FAK contains hardware and software for switches, routers, VPN, and WAN equipment and associated spares.

The contractor shall support USACE's emergency response mission by providing emergency response IT services within the scope of this requirement and related emergency event planning and support to USACE. Deployed personnel shall have privileged access to USACE systems.

The contractor is required to have staff in travel status within 12 hours of Government notification and approval both OCONUS and CONUS. The contractor is expected to make all travel arrangements and be prepared to work as long as it takes in potentially austere environments.

## SECTION D – PACKAGING AND MARKING

This page intentionally left blank

## SECTION E - INSPECTION AND ACCEPTANCE

### **E.1 PLACE OF INSPECTION AND ACCEPTANCE**

Inspection and acceptance of all work performance, reports, and other deliverables under this TO will be performed by the FEDSIM COR and USACE TPOC at USACE Headquarters, 441 G St. NW, Washington, DC 20226.

### **E.2 SCOPE OF INSPECTION**

All deliverables will be inspected for content, completeness, accuracy, and conformance to TO requirements by the FEDSIM COR and USACE TPOC. Inspection may include validation of information or software through the use of automated tools, testing, or inspections of the deliverables, as specified in the TO. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.

The Government requires a period NTE 15 workdays after receipt of deliverable items for inspection and acceptance or rejection.

### **E.3 BASIS OF ACCEPTANCE**

The basis for acceptance shall be compliance with the requirements set forth in the TO and relevant terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

Acceptance will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government have been resolved, through documentation updates, program correction, or other mutually agreeable methods.

Reports, documents, and narrative-type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected. If the deliverable is adequate, the Government may accept it or provide comments for incorporation.

All of the Government's comments on deliverables shall either be incorporated in the succeeding version of the deliverable, or the contractor shall explain to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a deliverable contains spelling errors, grammatical errors, or improper format, or otherwise does not conform to the quality assurance requirements stated within this TO, the document may be rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable version, the contractor shall arrange a meeting with the FEDSIM COR.

### **E.4 DELIVERABLES**

The Government will provide written acceptance, comments, and/or change requests, if any, within 15 workdays (unless specified otherwise in Section F) from Government receipt of the deliverable. Upon receipt of the Government comments, the contractor shall have ten workdays to incorporate the Government's comments and/or change requests and to resubmit the deliverable.

TO 47QFCA21F0001  
P00024

PAGE E-1

## SECTION E - INSPECTION AND ACCEPTANCE

### **E.5 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT**

The FEDSIM CO or FEDSIM COR will provide written notification of acceptance or rejection (**Section J, Attachment H**) of all deliverables within 15 workdays (unless specified otherwise in Section F). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

### **E.6 NON-CONFORMING PRODUCTS OR SERVICES**

Non-conforming products or services will be rejected. Deficiencies shall be corrected, by the contractor, within ten workdays of the rejection notice. If the deficiencies cannot be corrected within ten workdays, the contractor shall immediately notify the FEDSIM COR of the reason for the delay and provide a proposed corrective action plan within ten workdays.

If the contractor does not provide products or services that conform to the requirements of this TO, the Government will document the issues associated with the non-conforming products or services in the Award Fee Evaluation Board (AFEB) Report, and there will be an associated impact to the potential award fee earned.

## SECTION F – DELIVERIES OR PERFORMANCE

### **F.1 PERIOD OF PERFORMANCE (PoP)**

The PoP for this TO is a one-year Base Period, followed by four, one-year Option Periods:

Base Period:	28 December 2020 – 27 December 2021
First Option Period:	28 December 2021 – 27 December 2022
Second Option Period:	28 December 2022 – 27 December 2023
Third Option Period:	28 December 2023 – 27 December 2024
Fourth Option Period:	28 December 2024 – 27 December 2025

### **F.2 PLACE OF PERFORMANCE**

Place of performance is the contractor site with limited availability at Government locations, both CONUS and OCONUS. Contractor space availability in federally owned space is limited, evolving, and subject to change during TO performance. The contractor shall coordinate with and obtain government approval prior to any Federal space utilization. USACE OCIO/G-6 is headquartered at 441 G St. NW, Washington, DC 20226. Long-distance travel is anticipated to be required in support of this effort.

### **F.3 TASK ORDER (TO) SCHEDULE AND MILESTONE DATES**

The following schedule of milestones will be used by the FEDSIM COR to monitor timely progress under this TO.

The following abbreviations are used in this schedule:

- DEL: Deliverable
- IAW: In Accordance With
- NLT: No Later Than
- TOA: Task Order Award
- All references to days: Calendar Days

Deliverables are due the next Government workday if the due date falls on a holiday or weekend.

Data Rights Clause - Abbreviations in the Gov't Rights column of the table below shall be interpreted as follows:

UR: Unlimited Rights, per FAR 27.404-1(a) and Defense Federal Acquisition Regulation Supplement (DFARS) 252.227-7013

For software or documents that may be either proprietary Commercial Off-the-Shelf (COTS) or custom, RS/LD rights apply to proprietary COTS software or documents and UR rights apply to custom software or documents. The Government asserts UR rights to open source COTS software. Any collateral agreements (within the meaning of FAR 52.227-14) proposed for data, regardless of the type of rights offered, shall be subject to the requirements of TOR Section H.17.1 and H.17.2. For purposes of the foregoing, the terms “collateral agreement,” “Supplier Agreement,” and “Commercial Supplier Agreement” have the same meaning.

TO 47QFCA21F0001  
P00024

PAGE F-1

## SECTION F – DELIVERIES OR PERFORMANCE

The Government does not assert any rights to management software tools if the contractor does not plan to charge the Government directly for that tool and does not propose that the Government will own or use that tool.

The contractor shall deliver the deliverables listed in the following table on the dates specified:

<b>DEL. #</b>	<b>MILESTONE / DELIVERABLE</b>	<b>CLIN</b>	<b>TOR REFERENCE</b>	<b>DATE OF COMPLETION / DELIVERY</b>	<b>GOV'T RIGHTS</b>
	Project Start (PS)	1		December 28, 2020	N/A
1	Program Kick-Off Meeting	1	C.5.1.2	Within 25 workdays of PS	N/A
2	Program Kick-Off Meeting Agenda	1	C.5.1.2	At least three workdays prior to the Program Kick-Off Meeting	UR
3	Transition-In Plan	1	C.5.1.2, C.5.1.8	Due at Program Kick-Off Meeting	UR
4	Quality Management Plan (QMP)	X001	C.5.1.2, C.5.1.7	Due at Program Kick-Off Meeting; updated as changes in program processes are identified	UR
5	Service Integration and Management (SIAM) Plan	X001	C.5.1.2, C.5.1.12	Due at Program Kick-Off Meeting; updated as changes in program processes are identified	UR



## SECTION F – DELIVERIES OR PERFORMANCE

6	Cyber Security Management Plan (CSM)	X001	C.5.1.2	Due at Program Kick-Off Meeting; updated as changes in program processes are identified	UR
7	Proposed Task Order Portal	X001	C.5.1.2, C.5.1.13	Design due at Program Kick-Off Meeting. Fully Operational PS+ 90. Continuously updated as needed.	UR
8	Program Kick-Off Meeting Minutes Report	1	C.5.1.2	NLT 3 workdays following Program Kick-Off Meeting	UR
9	Program Management Review	X001	C.5.1.3	Monthly, 2 workdays prior to Monthly Program Review Meeting (Deliverable 10)	UR
10	Monthly Program Review Meeting	X001	C.5.1.3	Monthly, 10th calendar day of the next month)	N/A
11	Monthly Program Review Meeting Minutes	X001	C.5.1.3	5 workdays after Monthly Technical Status Meeting	UR
12	Technical Exchange Meeting Minutes	X002	C.5.1.4	6 workdays after Monthly Technical Exchange Meeting	UR

## SECTION F – DELIVERIES OR PERFORMANCE

13	Project Management Plan (PMP)	X001	C.5.1.5	Due at Kick-Off Meeting; updates as project changes occur, no less frequently than annually	UR
14	Trip Reports	X001	C.5.1.6	As required	UR
15	Transition-Out Plan	X003	C.5.1.9	Due six months prior to the end of the period of performance; updated annually	UR
16	IT Governance Documentation	X001	C.5.1.12	As requested	UR
17	Technical Direction Plan	X001	C.5.1.13	As requested, updated at a minimum annually or as changes occur	UR
18	Project Closeout Form	X001	C.5.1.13	Within 10 workdays of project closeout	UR
19	TDP Kickoff Meeting and Meeting Agenda	X001	C.5.1.13	If required, three workdays before TDP Kickoff Meeting	UR
20	TDP Kick-off Meeting Minutes Report	X001	C.5.1.13	If required, three workdays after the TDP Kick-Off Meeting	UR

## SECTION F – DELIVERIES OR PERFORMANCE

21	As A Service Assessment, Recommendation and Implementation Plan	X001	C.5.2	As required	UR
22	Turnkey Inside Plant Solution	X001	C.5.2.5	As required	UR
23	Systems Engineering Management Plan (SEMP)	X001	C.5.3.2	Within 90 days of PS; updated as necessary but no less than annually.	UR
24	Training Plan	X001	C.5.3.4	As required	UR
25	Technical Baselines and Integrated Architecture Products	X001	C.5.3.5	As required; update as changes occur	UR
26	Annual Configuration Audit	X001	C.5.3.5	Annually	UR
27	Design Documentation	X001	C.5.3.5	As required	UR
28	Hardware/Software Specifications, including BOM	X001	C.5.3.5	As required	UR
29	As-Built and Network Topology drawings	X001	C.5.3.5	As required	UR
30	Software Engineering Source Code	X001	C.5.3.7	As required	UR
31	Asset Management Plan	X001	C.5.3.8	PS + 90; annually thereafter	UR

## SECTION F – DELIVERIES OR PERFORMANCE

32	Configuration Management Implementation Plan	X001	C.5.3.8	PS + 90; annually thereafter	UR
33	License Agreement Management and Tracking Procedures	X001	C.5.3.9	PS + 90; annually thereafter	UR
34	Cybersecurity Strategy Plan (CSP)	X001	C.5.4	PS + 90; annually thereafter	UR
35	Conduct, Analyze, Address or Mitigate Cyber Scans	X001	C.5.4.1	As required	UR
36	POA&M, OIS, or Waivers	X001	C.5.4.1	As required	UR
37	STIG and IAVM Status	X001	C.5.4.1	As required	UR
38	Cyber Posture, Program and Capabilities Assessment	X001	C.5.4.2	As required	UR
39	IDS/IPS Test Plans, Operational Procedures and Maintenance Plans	X001	C.5.4.3	As required	UR
40	Access to asset reporting	X001	C.5.4.3	As required	UR
41	Recommendation Report	X001	C.5.4.3	As required	UR
42	Defensive Weakness and Vulnerability Report	X001	C.5.4.3	As required	UR

## SECTION F – DELIVERIES OR PERFORMANCE

43	Cyber After Action Reports	X001	C.5.4.3	As required	UR
44	Cyber sensor feed outage AAR	X001	C.5.4.4	As required	UR
45	Feeds, Sensors and Connectors reports	X001	C.5.4.4	As required	UR
46	COOP/DR Plan	X001	C.5.4.5	PS + 90; annually thereafter	UR
47	Cyber tools supporting documents, including maintenance schedules	X001	C.5.4.6	As required	UR
48	Threat Intelligence analysis	X001	C.5.4.7	As required	UR
49	Enterprise DAT and VSE Versioning	X001	C.5.4.8	As required	UR
50	DMZ web servers annual report	X001	C.5.4.9	Annually	UR
51	Pen-Testing Results Analysis	X001	C.5.4.10	As required	UR
52	Security Control Artifacts	X001	C.5.4.12	As required	UR
53	Security State Assessment	X001	C.5.4.12	As required	UR
54	Spillage Reporting	X001	C.5.4.2.13	As required	UR
55	Spillage POAM	X001	C.5.4.2.13	As required	UR
56	Telecommunications Management Plan	X001	C.5.5	As required, but at a minimum annually	UR

TO 47QFCA21F0001  
P00024

PAGE F-7

## SECTION F – DELIVERIES OR PERFORMANCE

57	Innovations	X001	C.5.6	As required	UR
58	Copy of TO (initial award and all modifications)	X001	F.4	Within 10 workdays of TOA	N/A
59	Government Property Reports	X001	H.3	Quarterly	UR
60	OPSEC Plan	X001	H.5.1	Within 90 days of PS; updates as required	UR
61	Relocation SOP	X001	H.13.24	Within 180 days of PS; update as required	
62	Living Quarters Allowance (LQA) SOP	X001	H.13.25.1	Within 180 days of PS; update as required	UR
63	LQA Reconciliation	X001	H.13.25.1	Annually if employees qualified for LQA in the previous calendar year	UR

**The contractor shall mark all deliverables listed in the above table to indicate authorship by contractor (i.e., non-Government) personnel; provided, however, that no deliverable shall contain any proprietary markings inconsistent with the Government's data rights set forth in this TO. The Government reserves the right to treat non-conforming markings in accordance with DFARS 252.227-7013 and 252.227-7014.**

### **F.4 PUBLIC RELEASE OF CONTRACT DOCUMENTS REQUIREMENT**

The contractor agrees to submit, within ten workdays from the date of the FEDSIM CO's execution of the initial TO, or any modification to the TO (exclusive of Saturdays, Sundays, and Federal holidays), a Portable Document Format (PDF) file of the fully executed document with all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of GSA (**Section F, Deliverable 58**). The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 United States Code (U.S.C.) § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b) (4), shall explain why the information is considered to be a trade secret or commercial or

TO 47QFCA21F0001  
P00024

## SECTION F – DELIVERIES OR PERFORMANCE

financial information that is privileged or confidential. Information provided by the contractor in response to the contract requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA.

GSA will carefully consider the contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

### **F.5 DELIVERABLES MEDIA**

The contractor shall deliver all electronic versions by email, TO Management Portal or removable electronic media, as well as placing in the USACE designated repository. The following are the required electronic formats, whose versions must be compatible with the latest, commonly available version in use by USACE.

- |                 |                          |
|-----------------|--------------------------|
| a. Text         | Microsoft (MS) Word, PDF |
| b. Spreadsheets | MS Excel                 |
| c. Briefings    | MS PowerPoint            |
| d. Drawings     | MS Visio                 |
| e. Schedules    | MS Project               |

### **F.6 PLACE(S) OF DELIVERY**

Copies of all deliverables shall be delivered to the FEDSIM COR at the following address:

GSA FAS AAS FEDSIM  
ATTN: FEDSIM COR (QF0B)  
1800 F Street, NW  
Washington, D.C. 20405  
Telephone: (202) 357-9538  
Email: kevin.mentrikoski@gsa.gov

Copies of all deliverables shall also be delivered to the USACE TPOC. The USACE TPOC name, address, and contact information will be provided at award.

### **F.7 NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT (PNR)**

The contractor shall notify the FEDSIM COR via a PNR (**Section J, Attachment E**) as soon as it becomes apparent to the contractor that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The FEDSIM COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

## SECTION G – CONTRACT ADMINISTRATION DATA

### **G.1 CONTRACTING OFFICER’S REPRESENTATIVE (COR)**

The FEDSIM CO appointed a FEDSIM COR in writing through a COR Appointment Letter (**Section J, Attachment A**). The FEDSIM COR will receive, for the Government, all work called for by the TO and will represent the FEDSIM CO in the technical phases of the work. The FEDSIM COR will provide no supervisory or instructional assistance to contractor personnel.

The FEDSIM COR is not authorized to change any of the terms and conditions, scope, schedule, and price of the Contract or the TO. Changes in the scope of work will be made only by the FEDSIM CO by properly executed modifications to the Contract or the TO.

#### **G.1.1 CONTRACT ADMINISTRATION**

Contracting Officer:

Michelle Dunn  
GSA FAS AAS FEDSIM (QF0B)  
1800 F Street, NW  
Washington, D.C. 20405  
Telephone: (404) 860-0503  
Email: michelle.dunn@gsa.gov

Contracting Officer’s Representative:

Kevin Mentrikoski  
GSA FAS AAS FEDSIM (QF0B)  
1800 F Street, NW  
Washington, D.C. 20405  
Telephone: (202) 357-9538  
Email: kevin.mentrikoski@gsa.gov

Kadijat Oladiran  
GSA FAS AAS FEDSIM (QF0B)  
1800 F Street, NW  
Washington, D.C. 20405  
Telephone: (202) 304-2359  
Email: kadijat.oladiran@gsa.gov

Assistant Contracting Officer’s Representative:

None

Property Administrator:

Colin O’Connor  
GSA FAS AAS FEDSIM (QF0B)  
1800 F Street, NW

TO 47QFCA21F0001  
P00024

PAGE G-1



SECTION G – CONTRACT ADMINISTRATION DATA

Washington, D.C. 20405  
Telephone: (813) 499-7653  
Email: colin.oconnor@gsa.gov

Henry Pielact  
GSA FAS AAS FEDSIM (QF0B)  
1800 F Street, NW  
Washington, D.C. 20405  
Telephone: (202) 615-4769  
Email: henry.pielact@gsa.gov

Operations Technical Point of Contract:

(b) (6)

CIO Technical Point of Contract:

(b) (6)

Assistant Technical Point of Contact:

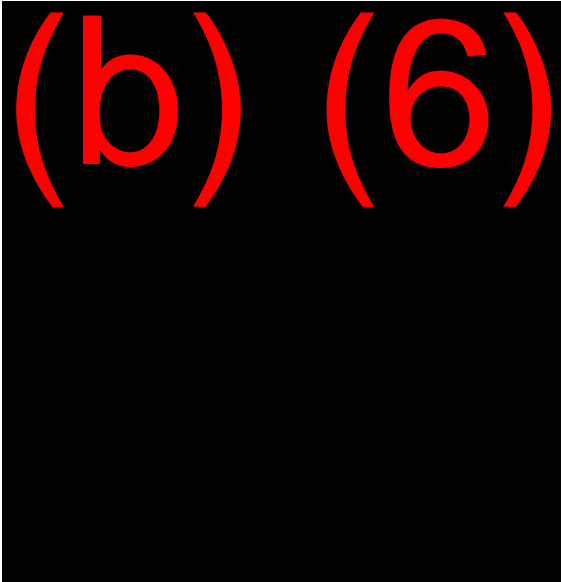
(b) (6)

Sharon Freitas  
CEIT-BMA  
Building 230 Otake Street

TO 47QFCA21F0001  
P00024

PAGE G-2

## SECTION G – CONTRACT ADMINISTRATION DATA



### **G.2 INVOICE SUBMISSION**

The contractor shall submit Requests for Payments in accordance with the format contained in General Services Administration Acquisition Manual (GSAM) 552.232-25, PROMPT PAYMENT (NOV 2009), to be considered proper for payment. In addition, the following data elements shall be included on each invoice:

Task Order Number: *(from GSA Form 300, Block 2)*

Paying Number: *(ACT/DAC NO.) (From GSA Form 300, Block 4)*

FEDSIM Project Number: CR0182

Project Title: USACE RITS

The contractor shall submit invoices as follows:

The contractor shall utilize FEDSIM's electronic Assisted Services Shared Information System (ASSIST) to submit invoices. The contractor shall manually enter CLIN charges into Central Invoice Services (CIS) in the ASSIST Portal. Summary charges on invoices shall match the charges listed in CIS for all CLINs. The contractor shall submit invoices electronically by logging onto the following link (requires Internet Explorer to access the link):

<https://portal.fas.gsa.gov>

Log in using your assigned Identification (ID) and password, navigate to the order against which you want to invoice, click the Invoices and Acceptance Reports link in the left navigator, and then click the *Create New Invoice* button. By utilizing this method, no paper copy of the invoice shall be submitted to GSA FEDSIM or the GSA Finance Center. The contractor shall provide invoice backup data, as an attachment to the invoice, in accordance with the contract type, including detail such as labor categories, rates, and quantities of labor hours per labor category. The FEDSIM COR may require the contractor to submit a written "hardcopy" invoice with the

## SECTION G – CONTRACT ADMINISTRATION DATA

client's certification prior to invoice payment. A paper copy of the invoice is required for a credit.

The contractor is certifying, by submission of an invoice in the CIS, that the invoice is correct and proper for payment.

If there are any issues submitting an invoice, contact the Assisted Acquisition Services Business Systems (AASBS) Help Desk for support at 877-472-4877 (toll free) or by email at [AASBS.helpdesk@gsa.gov](mailto:AASBS.helpdesk@gsa.gov).

### **G.3 INVOICE REQUIREMENTS**

The contractor shall submit a draft copy of an invoice backup in Excel to the FEDSIM COR and USACE TPOC for review prior to its submission to ASSIST. The draft invoice shall not be construed as a proper invoice in accordance with FAR 32.9 and GSAM 532.9. The contractor shall provide receipts on an as-requested basis.

The final invoice is desired to be submitted within six months of project completion. Upon project completion, the contractor shall provide a final invoice status update monthly.

Regardless of contract type, the contractor shall report the following data:

- a. Governmentwide Acquisition Contract (GWAC) Number
- b. Task Order Award Number (NOT the Solicitation Number).
- c. Contractor Invoice Number.
- d. Contractor Name.
- e. POC Information.
- f. Current PoP.
- g. Amount of invoice that was subcontracted.

The amount of invoice that was subcontracted to a small business shall be made available upon request.

#### **G.3.1 COST-PLUS-AWARD-FEE (CPAF) CLINs (for LABOR)**

The contractor may invoice monthly on the basis of cost incurred for the CPAF CLINs. The invoice shall include the PoP covered by the invoice (all current charges shall be within the active PoP) and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in Section B), by contractor employee, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

- a. Employee name (current and past employees).
- b. Employee Company.
- c. Employee Alliant labor category.
- d. Current monthly and total cumulative hours worked.
- e. Direct Labor Rate.

TO 47QFCA21F0001  
P00024

PAGE G-4

## SECTION G – CONTRACT ADMINISTRATION DATA

- f. Corresponding proposed ceiling rate.
- g. Effective hourly rate (e.g., cumulative costs/cumulative hours).
- h. Current approved billing rate percentages in support of costs billed.
- i. Itemization of cost centers applied to each individual invoiced.
- j. Itemized breakout of indirect costs (e.g., Fringe, Overhead (OH), General and Administrative (G&A) burdened costs for each individual invoiced (rollups are unacceptable)).
- k. Any cost incurred not billed by CLIN (e.g., lagging costs).
- l. Labor adjustments from any previous months (e.g., timesheet corrections).
- m. Provide comments for deviation outside of 5 percent.
- n. Financial tracking data as necessary to meet USACE and FEDSIM cost tracking requirements (i.e., tracking at the division/site/project, Task/Subtask, ACE Work Center and or TDL level).

All cost presentations provided by the contractor in Excel shall show indirect charges itemized by individual with corresponding indirect rates with cost center information. The invoice detail shall be organized by CLIN.

The contractor may invoice for fee after accepting the modification which includes the award fee determination and any corresponding deobligation of unearned fee. See the AFDP in **Section J, Attachment D** for additional information on the award fee determination process.

When the Incurred Cost method is used to determine the Award Fee Pool Allocation for an Award Fee period, the incurred cost shall be calculated using approved provisional billing rates as established by the cognizant Government auditor, in accordance with FAR 42.704. Approved provisional billing rates shall not be adjusted for the purpose of accumulating incurred costs and calculating the Award Fee Pool Allocation.

### **G.3.2 TOOLS AND OTHER DIRECT COSTS (ODCs)**

The contractor may invoice monthly on the basis of cost incurred for the Tools and ODC CLINs. The invoice shall include the PoP covered by the invoice and the CLIN number and title. In addition, the contractor shall provide the following detailed information for each invoice submitted, as applicable. Spreadsheet submissions are required.

- a. Tools and/or ODCs purchased.
- b. Request to Initiate Purchase (RIP) or Consent to Purchase (CTP) number or identifier.
- c. Date accepted by the Government.
- d. Associated CLIN.
- e. Project-to-date totals by CLIN.
- f. Cost incurred not billed by CLIN.
- g. Remaining balance of the CLIN.
- h. Any applicable Fee

## SECTION G – CONTRACT ADMINISTRATION DATA

- i. Financial tracking data as necessary to meet USACE and FEDSIM cost tracking requirements (i.e., tracking at the division/site/project, Task/Subtask, ACE Work Center and or TDL level).

All cost presentations provided by the contractor shall also include any indirect costs being applied with associated cost center information.

### **G.3.3 TRAVEL**

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

- a. Federal Travel Regulation (FTR) - prescribed by the GSA, for travel in the contiguous U.S.
- b. Joint Travel Regulations (JTR) Volume 2, Department of Defense (DoD) Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska (AK), Hawaii (HI), and outlying areas of the U.S.
- c. Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State (DoS), for travel in areas not covered in the FTR or JTR.

The contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the JTR, FTR, or DSSR as applicable. The invoice shall include the PoP covered by the invoice and the CLIN number and title. Separate worksheets, in MS Excel format, shall be submitted for travel.

CLIN and Task Total Travel: This invoice information shall identify all cumulative travel costs billed by CLIN and Task. The current invoice period's travel details shall include separate columns and totals and include the following:

- a. Travel Authorization Request (TAR) number or identifier, approver name, and approval date.
- b. Current invoice period.
- c. Names of persons traveling.
- d. Number of travel days.
- e. Dates of travel.
- f. Number of days per diem charged.
- g. Per Diem rate used.
- h. Total per diem charged.
- i. Transportation costs.
- j. Total charges.
- k. Explanation of variances exceeding ten percent of the approved versus actual costs.
- l. Indirect handling rate.

## SECTION G – CONTRACT ADMINISTRATION DATA

- m. Financial tracking data as necessary to meet USACE and FEDSIM cost tracking requirements (i.e., tracking at the division/site/project, Task/Subtask, ACE Work Center and or TDL level).

All cost presentations provided by the contractor shall also include OH charges and G&A charges in accordance with the contractor's Defense Contract Audit Agency (DCAA) cost disclosure statement.

### **G.4 TASK ORDER (TO) CLOSEOUT**

The Government will unilaterally close out the TO no later than six years after the end of the TO PoP if the contractor does not provide final DCAA rates by that time.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

### **H.1 KEY PERSONNEL**

The following are the minimum personnel who shall be designated as “Key.” The Government does not intend to dictate the composition of the ideal team to perform this TO. In addition to those Key Personnel described below, the Government will consider no more than three additional Key Personnel for which the offeror shall provide its own required/desired qualifications. The Key Personnel shall possess all required qualifications at time of proposal submission.

- a. Program Manager (PM)
- b. Cybersecurity Operations Manager
- c. Operations Manager
- d. Transformation/Process Improvement Subject Matter Expert (SME)
- e. Resource Manager

The Government desires that Key Personnel be assigned for the duration of the TO.

#### **H.1.1 PROGRAM MANAGER (PM)**

The contractor shall identify a Program Manager (PM) by name who shall provide management, direction, administration, quality assurance (as defined in **Section C.5.1**), and leadership of the execution of this TO.

This person shall be located on-site at the Government Accountability Office (GAO) Building in Washington, D.C., and may be required to occasionally travel to CONUS and OCONUS locations in support of the TO.

It is required that the PM has the following qualifications:

- a. A minimum of ten years of experience with the management of an Enterprise IT Service Delivery and Management Program similar to the requirements of this TOR.
- b. Five years of experience with the management, manpower utilization, and supervision of employees (including subcontractors) of various labor categories and skills in projects similar in scope as proposed for this TOR.
- c. Project Management Professional (PMP) or Program Management Professional (PgMP) Certification issued from the Project Management Institute (PMI).
- d. An active Secret security clearance.

It is desired that the PM has the following qualifications:

- a. Five years of experience developing a strategic vision for a complex organization, balancing modernization needs with critical daily operations and maintenance requirements.
- b. Five years of experience managing programs or projects in a DoD environment.
- c. Five years of experience with the Federal procurement process.
- d. Five years of experience with the administration of cost-type contracts.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

- e. ITIL® v3 Practitioner or ITIL® V4 equivalent.

### **H.1.2 CYBERSECURITY OPERATIONS MANAGER**

The Cybersecurity Operations Manager shall manage all cybersecurity operations and related processes based on Government-approved ITSM processes consistent with industry best practices. The Cybersecurity Operations Manager is tasked with overall leadership of TO governance, risk, and compliance and ensuring operations sets, comply, and monitor in accordance with regulations, policies, and processes.

It is required that the Cybersecurity Operations Manager has the following qualifications:

- a. A minimum of five years of experience with all phases of IA and accreditation processes, securing IT systems and services using Government and industry IA standards, policies, guidelines, and best practices.
- b. Five years of experience managing and leading a security operations staff with skills applicable to a project environment similar in size and scope referenced in this TO.
- c. Five years of experience successfully managing information security risks to include completing the entire Access and Authorize (A&A) process including receiving ATO for the cloud.
- d. Possesses a Certified Information Systems Security Professional certification or approved equivalent current DoD 8570 Information Assurance Management (IAM) Level II certification.
- e. An active Top Secret (TS)/Sensitive Compartmented Information (SCI) security clearance.

It is desired that the Cybersecurity Operations Manager has the following qualifications:

- a. Five years of experience with encryption devices and procedures as they relate to networks and data.
- b. Five years of experience with Federal governance, risk, and compliance management.
- c. ITIL® v3 Practitioner or ITIL® V4 equivalent.

### **H.1.3 OPERATIONS MANAGER**

The Operations Manager shall be responsible for the delivery of IT service and projects from engineering to operations, shall be the service owner for all end-user and customer-facing IT services and solutions, and shall ensure end-to-end delivery of services based on Government-approved ITSM processes consistent with industry best practices. The Operations Manager shall lead the analysis, planning, and implementation of ITSM initiatives in support of USACE operations and ensure its alignment with industry best practices and ITIL approaches. The Operations Manager shall identify IT operational requirements, provide day-to-day leadership and quality control, and provide expertise on best practices to continually improve the USACE implementation of ITIL practices with the goal of exceeding performance objectives and reducing costs and schedule. Additionally, the Operations Manager shall serve as the patch and



## SECTION H – SPECIAL CONTRACT REQUIREMENTS

device configuration lead, ensuring that all USACE-supported devices and systems are configured and have installed the latest patches to meet all cybersecurity and operational requirements.

It is required that the Operations Manager has the following qualifications:

- a. ITIL®V3 Expert Level Certification or ITIL® V4 equivalent.
- b. Five years of experience in managing Enterprise IT operations similar in scope, to the requirements of this TO, including implementation of ITIL best practices.
- c. An active Secret security clearance.

It is desired that the Operations Manager has the following qualifications:

- a. Possesses a current DoD 8570 IAM level I Certification.
- b. Five years of experience managing the device configuration and patch management for an enterprise operation of a similar size, scope, and complexity.
- c. Five years of experience managing service desk teams and supporting a requirement that is similar in size, scope, and complexity to this TOR.
- d. Five years of experience in communicating with Government personnel, including agency executives.
- e. Five years of experience providing performance-based customer service support against multiple performance metrics in the Federal marketplace.

### **H.1.4 TRANSFORMATION/PROCESS IMPROVEMENT SUBJECT MATTER EXPERT (SME)**

The Transformation/Process Improvement SME shall be responsible for the delivery of transformation services and process improvement to improve the IT posture of USACE from its current state to a modern ITIL/ITSM-supported service delivery model. The Transformation/Process Improvement SME shall lead the development of modern service offerings and process improvements, including, but not limited to, the development of cloud environments, SaaS, Device-as-a-Service, and automation. The Transformation/Process Improvement SME shall review current process and recommend improvements to provide additional benefits to USACE OCIO G6. Additionally, the Transformation SME shall recommend metrics to the Government for review to support the continual improvement of TO performance. The Transformation/Process Improvement SME shall be responsible for the design and development of cloud solutions, as well as managing the divestiture of current infrastructure and applications as they are replaced by cloud solutions.

It is required that the Transformation/Process Improvement SME has the following qualifications:

- a. AWS Certified Solutions Architect, Cisco Certified Network Associate (CCNA)/ Cisco Certified Network Professional (CCNP) or Microsoft Certified Solutions Expert (MSCE) or similar commercial cloud platform or infrastructure certification.
- b. Five years of experience leading cloud migration and divestitures.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

- c. Five years of experience leading transformation projects in the Federal environment.
- d. Five years of experience leading organizational change resulting in improved performance outcomes.

It is desired that the Transformation/Process Improvement SME has the following qualifications:

- a. ITIL® V3 Practitioner or ITIL® V4 equivalent.
- b. Five years of experience implementing Software as a service (SaaS) offerings in the Federal environment.
- c. Five years of experience implementing device as a service in the Federal environment.
- d. Lean Six Sigma Black Belt.

### **H.1.5 RESOURCE MANAGER**

The Resource Manager shall be responsible for the delivery of TO financials to support the USACE cost and financial objectives. The Resource Manager shall implement processes and procedures to ensure costs are captured accurately and tracked to the appropriate level of granularity to meet USACE requirements. The Resource Manager shall establish processes necessary to achieve Technology Business Model (TBM) frameworks and allow USACE the ability to provide its customers with a consumption billing model for services provided.

It is required that the Resource Manager has the following qualifications:

- a. Five years of experience leading the cost and financial tracking for a project of similar size, scope, and complexity.

It is desired that the Resource Manager has the following qualifications:

- a. ITIL®V3 Practitioner or ITIL® V4 equivalent.
- b. Two years of experience providing the TBM framework for a Federal client.
- c. Five years of experience implementing consumption-based billing models.

### **H.2 KEY PERSONNEL SUBSTITUTION**

The contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the FEDSIM CO. Prior to utilizing other than the Key Personnel specified in its proposal in response to the TOR, the contractor shall notify the FEDSIM CO and the FEDSIM COR. This notification shall be no later than 10 calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.

Substitute Key Personnel qualifications shall be equal to, or greater than, those of the Key Personnel substituted. If the FEDSIM CO and the FEDSIM COR determine that a proposed substitute Key Personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the contractor may be subject to default action as prescribed by FAR 52.249-6 Termination.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

### **H.3 GOVERNMENT-FURNISHED PROPERTY (GFP)**

The Government will review, authorize, and provide GFP and GFE in support of this TO. The contractor shall properly handle, transport, operate, maintain, track, account for, and control all GFP (**Section F, Deliverable 59**) in accordance with the following:

- a. FAR 52.245-1, Government Property
- b. DFARS 252.245-7002, Reporting Loss of Government Property
- c. AR 735-5, Property Accountability Policies

All GFP shall be returned to the Government at the end of this TO or at any time by written notice.

Within USACE spaces, the Government will provide adequate physical work space and will furnish GFP as required by the position, when requested by the contractor, and approved by the Government; GFP may include a desk, phone, computer equipment (including all necessary hardware and software), an email account, and use of the Government telephone, facsimile machine, and copier. The Government will provide access to required software environments.

#### **H.3.1 PURCHASING VIA COMPUTER HARDWARE ENTERPRISE AND SOFTWARE SOLUTIONS (CHESS)**

All purchases shall be consistent with DoD and Army Acquisition Policies. When procuring COTS software, desktops, notebook computers, video teleconferencing, or other commercial IT equipment (e.g., routers, servers, and printers), the contractor shall use the CHESS to the maximum extent possible.

### **H.4 GOVERNMENT-FURNISHED INFORMATION (GFI)**

The Government will review, authorize, and provide GFI/Government-furnished publications in support of this TO. If additional GFI is necessary that the contractor cannot otherwise obtain, the contractor shall document the information and publications necessary to accomplish the tasks outlined in this TO.

Information will include reports, briefings, and other related reference material. The Government will provide the contractor with timely information, including access to unclassified and classified Government information networks and will facilitate contractor personnel interfaces with other DoD staff, service staff, and USACE customers and stakeholders, as required, to complete the requirements associated with this TO.

Use of GFI for other than Government work is strictly prohibited.

### **H.5 SECURITY REQUIREMENTS**

The USACE TPOC will have the Industrial Security Specialist review the DD 254 before it is approved (**Section J, Attachment J**). The contractor shall submit all proposed subcontractor DD 254s to the USACE TPOC for review and approval prior to issuance.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

All contractor and all associated subcontractor employees shall comply with applicable installation, facility, network, system, and/or area commander installation/facility access and local security policies and procedures (provided by Government representatives). The contractor shall also provide all information required for background checks to meet network, system, and installation/facility access requirements.

The contractor workforce shall comply with all personal identity verification requirements (FAR clause 52.204-9, Personal Identity Verification of Contractor Personnel) as directed by DoD, Headquarters Department of the Army (HQDA) and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the Force Protection Condition at any installation or facility change, the Government may require changes in contractor security matters or processes.

The contractor and all associated subcontractors shall receive a brief/training on the local suspicious activity reporting program. This locally developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the project manager, security representative, or law enforcement entity. This training shall be completed within 30 calendar days of Contract award and within 30 calendar days of new employees commencing performance with the results reported to the FEDSIM COR NLT five calendar days after the completion of the training.

All contractor employees with access to a Government information system shall be registered in the Army Training Certification Tracking System (ATCTS) at commencement of services, and shall successfully complete the DoD IA Awareness training prior to access to the information systems and then annually thereafter in accordance with personnel security standards listed in AR 25-2 (Information Assurance). An appropriate background investigation will also be conducted prior to accessing the Government information systems.

### **H.5.1 OPERATIONS SECURITY (OPSEC) REQUIREMENTS**

The contractor shall develop an unclassified OPSEC SOP/Plan within 90 calendar days of Contract award (**Section F, Deliverable 60**). The OPSEC SOP/Plan must be reviewed and approved by the RA OPSEC Officer. The SOP/Plan shall include the Government's critical information, why it needs to be protected, where it is located, who is responsible for it, and how to protect it. In addition, the contractor shall identify an individual who will be an OPSEC coordinator. All new contractor employees shall complete Level I OPSEC Training within 30 calendar days of their reporting for duty. Additionally, all contractor employees shall complete annual OPSEC awareness training. The contractor shall submit certificates of completion for each affected contractor and subcontractor employee, to the FEDSIM COR or to the FEDSIM Contracting Officer (CO) (if a COR is not assigned), within five calendar days after completion of training. OPSEC awareness training is available at the following websites: <https://www.iad.gov/ioss/> or <http://www.cdse.edu/catalog/operations-security.html>; or it can be provided by the RA OPSEC Officer in presentation form which will be documented via memorandum.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

All contractor employees shall ensure the following Antiterrorism (AT)/Operations Security (OPSEC) requirements are met prior to deploying personnel authorized to accompany U.S. Armed Forces outside the U.S.; to include compliance with laws, regulations, pre-deployment requirements, and required training in accordance with combatant command guidance.

### **H.5.2 INFORMATION ASSURANCE (IA)**

The contractor may have access to sensitive (including privileged and confidential) data, information, and materials of the U.S. Government. These printed and electronic documents are for internal use only and remain the sole property of the U.S. Government. Some of these materials are protected by the Privacy Act of 1974 (amended) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.

All contractor employees supporting IA/IT functions shall be appropriately certified upon Contract award in accordance with DoD 8570.01-M, DFARS 252.239-7001, AR 25-2, or any successor policies or regulations. The baseline certification as stipulated in DoD 8570.01-M shall be completed upon Contract award.

Additionally, all contractor personnel shall meet the following background investigation based on the assigned position risk level:

- a. IT Level III - Contractor personnel shall possess a Tier 1 background investigation.
- b. IT level II - Contractor personnel shall possess a Tier 3 background investigation.
- c. IT Level I - Contractor personnel shall possess a Tier 5 background investigation.

The contractor shall coordinate all requests for investigations with the FEDSIM COR and USACE TPOC or other designated Government POC to ensure that each employee meets the criteria for determining the position sensitivity risk designation.

All contractor personnel shall receive a favorable preliminary Enter on Duty (EOD) determination prior to beginning work on this TO and prior to receiving initial access to USACE information systems. Contractor personnel shall receive a favorable final fitness determination prior to obtaining privileged IT access. If the results of a background investigation are not favorable, then all access shall be terminated.

The contractor, when notified of an unfavorable final fitness determination on a contractor employee, as determined by the Government, shall immediately remove the contract employee from the TO and revoke all access to facilities and IT systems. All credentials and access cards that were issued to the individual shall be returned to the Government POC.

The contractor shall be responsible for managing its workforce to ensure that sufficient contract personnel who meet all suitability requirements are available to perform the duties required under this TO. New or replacement contract personnel shall have previously received a favorable suitability determination in sufficient time to perform work and obtain full access to USACE IT systems.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

The contractor is responsible for all travel and labor costs associated with fingerprinting to meet background investigation requirements. Travel costs may include mileage, vehicle rental or other modes of transportation, per diem, and lodging.

The contractor shall ensure that roles/privileges granted to contractor personnel on USACE IT systems are commensurate with the roles/privileges and information access essential to that individual's performance of his/her assignments. These roles/privileges can be limited or revoked by the Government.

Failure to comply with the contractor personnel security investigative requirements may result in termination of the Contract for default.

The contractor shall maintain a Contractor IA/IT status list via the contractor's management portal. At a minimum, the Contractor IA/IT list shall provide the following information:

- a. Contract employee name
- b. Contractor company
- c. Task area and job function
- d. Place of performance (city/state)
- e. Facility (contractor, Government, work-at-home)
- f. EOD date
- g. IA category and specialties (Information Assurance Technical (IAT), IAM, Computer Network Defense-Service Provider (CND-SPs), IA Workforce System Architecture and Engineering(IASAEs)) for position held
- h. IA level for position held
- i. Background investigation level required for position held
- j. Baseline certification status
- k. CE/OS certification status (if applicable)
- l. Background investigation adjudication date
- m. Additional information as required to validate contractor's IA/IT suitability

All contractor employees and associated subcontractor employees shall complete the DoD IA awareness training before issuance of network access and annually thereafter. All contractor employees working IA/IT functions shall comply with DoD and Army training requirements in DoD 8570.01, DoD 8570.01-M, and AR 25-2.

### **H.5.3 HANDLING OR ACCESS TO CLASSIFIED INFORMATION**

The contractor shall comply with FAR 52.204-2, Security Requirements. This clause involves access to information classified "Confidential," "Secret," or "Top Secret" and requires contractors to comply with 1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-M); and 2) any revisions to DoD 5220.22-M, notice of which has been furnished to the contractor.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

### **H.5.4 SECURITY CLEARANCES**

All contractors/subcontractors supporting this effort in CONUS (classified and unclassified portions) shall be U.S. citizens. All contractor personnel working on or managing this effort shall strictly adhere to USACE security regulations and procedures, including those encompassing responsibilities of possessing a clearance within Joint Personnel Adjudication System (JPAS). All members of the contractor team (e.g., prime contractor, subcontractors, etc.) providing personnel, including supervisory personnel, to perform the work shall comply with the applicable security clearance levels (facilities/personnel) based on the sensitivity of the task/work requiring a clearance.

The contractor shall comply with AR 380-67 (Personnel Security Program) and Homeland Security Presidential Directive-12 (HSPD-12) (Policy for a Common Identification Standard for Federal Employees and Contractors) as well as FAR 52.204-2, Security Requirements. Additionally, contractors shall comply with the Security Agreement (DD Form 441), including the NISPOM (DoD 5220.22-M); and any revisions to DoD 5220.22-M, notice of which has been furnished to the contractor. For classified contracts, the DD Form 254 will be attached with the contract.

All contractor employees shall complete annual Threat Awareness and Reporting Program (TARP) training provided by a counterintelligence agent, in accordance with AR 381-12. The contractor shall submit certificates of completion for each affected contractor and subcontractor employee(s) or a memorandum for the record, to the FEDSIM COR or to the FEDSIM CO (if a COR is not assigned), within five calendar days after completion of training. Authorized web-based TARP training for CAC holders is available at the following website:  
<https://www.us.army.mil/suite/page/655474>

The contractor shall pre-screen candidates using the E-Verify program (<http://www.uscis.gov/e-verify>) website to meet the established employment eligibility requirements. The contractor shall ensure that the candidate has two valid forms of Government issued identification prior to enrollment to ensure the correct information is entered into the E-Verify system. An initial list of verified/eligible candidates shall be provided to the FEDSIM COR no later than three workdays after the initial contract award. Please note that when contracts are with individuals, the individuals will be required to complete a Form I-9, Employment Eligibility Verification, with the designated Government representative. This form will be provided to the FEDSIM CO and shall become part of the official contract file.

The contractor and all subcontractor employees will be issued a CAC only if duties involve one of the following: 1) Both physical access to a DoD facility and access, via logon, to DoD networks on-site or remotely; 2) Remote access, via logon, to a DoD network using DoD-approved remote access procedures; or 3) Physical access to multiple DoD facilities or multiple non-DoD federally controlled facilities on behalf of the DoD on a recurring basis for a period of six months or more. At the discretion of the sponsoring activity, an interim CAC may be issued based on a favorable review of the Federal Bureau of Investigation (FBI) fingerprint check and a successfully scheduled National Agency Check with Inquiries (NACI) at the Office of Personnel Management (OPM). Contractor and all associated subcontractor employees shall comply with

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

adjudication standards and procedures using the National Crime Information Center Interstate Identification Index (NCIC-III) and Terrorist Screening Database (TSDB) (Army Directive 2014-05/AR 190-13), applicable installation, facility, and area commander installation/facility access and local security policies and procedures (provided by a Government representative, as NCIC and TSDB are available), or at OCONUS locations, in accordance with Status of Forces Agreements (SOFAs) and other theater regulations.

In general, all necessary facility and employee security clearances shall be at the expense of the contractor. The contractor shall comply with all security requirements.

### **H.6 FACILITY CLEARANCE LEVEL (FCL)**

The prime contractor company shall have a Facility Clearance (FCL) at the appropriate level (in accordance with the NISPOM DoD 5220.22-M and AR 380-49) prior to the start of the TO awarded PoP. Contractor personnel performing work under this Contract shall have the required security clearance, per AR 380-67, at the appropriate level at the start of the PoP. Security clearances and FCL requirements are required to be maintained for the life of the Contract in accordance with the DD Form 254 attached to the Contract. If the contractor does not have an FCL, USACE will sponsor the prime contract company's effort to obtain the FCL.

### **H.7 LOGISTICAL SUPPORT**

All non-local contracting personnel shall comply with theater clearance requirements and allow the combatant commander to exercise oversight to ensure the contractor's compliance with combatant commander and subordinate task force commander policies and directives.

All U.S.-based contractor employees and associated subcontractor employees traveling overseas will receive the Government-provided AOR specific AT awareness training. The documentation of training completion shall be provided to the FEDSIM COR prior to departure.

### **H.8 TRAINING AND PERMITS**

All contractor employees, to include subcontractor employees, requiring access to Army installations, facilities, or controlled access areas; or requiring network access, shall complete AT Level I awareness training within 30 calendar days after TO start date or effective date of employment for TO work, whichever is applicable. Upon request, the contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee, to the USACE TPOC, FEDSIM COR, or to the FEDSIM CO, within five calendar days after completion of training by all employees and subcontractor personnel. AT Level I awareness training is available at the following website: <http://jko.jten.mil/courses/atl1/launch.html>; or it can be provided by the RA ATO in a presentation which will be documented via memorandum.

#### **H.8.2 CONTROLLED UNCLASSIFIED INFORMATION (CUI) TRAINING**

All contractor employees, to include subcontractor employees are required to complete initial and annual refresher CUI training IAW DoDI 5200.48 or successor versions. Upon request, the



## SECTION H – SPECIAL CONTRACT REQUIREMENTS

contractor shall submit certificates of completion for each contractor employee and subcontractor employee.

### **H.9 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS**

#### **H.9.1 ORGANIZATIONAL CONFLICT OF INTEREST (OCI)**

If a contractor has performed, is currently performing work, or anticipates performing work that creates or represents an actual or potential OCI, the contractor shall immediately disclose this actual or potential OCI to the FEDSIM CO in accordance with FAR Subpart 9.5. The nature of the OCI may involve the prime contractor, subcontractors of any tier, or teaming partners.

#### **H.9.2 NON-DISCLOSURE REQUIREMENTS**

If the contractor acts on behalf of, or provides advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, then the contractor shall execute and submit a Corporate Non-Disclosure Agreement (NDA) Form (**Section J, Attachment L**) and ensure that all its personnel (including subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO:

- a. Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or proposal information, or source selection information.
- b. Are instructed in FAR Part 9 for third-party disclosures when acting in an advisory capacity.

All proposed replacement contractor personnel shall also be instructed in the requirements of FAR 3.104. Any information provided by contractors in the performance of this TO or obtained from the Government is only to be used in the performance of the TO. The contractor shall put in place appropriate procedures for the protection of such information and shall be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

### **H.10 SECTION 508 COMPLIANCE REQUIREMENTS**

Unless the Government invokes an exemption, all Electronic and Information Technology (EIT) products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, 29 U.S.C. 794d, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 Code of Federal Regulations (CFR) 1194. The contractor shall identify all EIT products and services provided, identify the technical standards applicable to all products and services provided, and state the degree of compliance with the applicable standards. Additionally, the contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The contractor must ensure that the list is easily accessible by typical users beginning at time of award.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

### **H.11 ADEQUATE COST ACCOUNTING SYSTEM**

The adequacy of the contractor's accounting system and its associated internal control system, as well as contractor compliance with the Cost Accounting Standards (CAS); affect the quality and validity of the contractor data upon which the Government must rely for its management oversight of the contractor and Contract performance. The contractor's cost accounting system shall be adequate during the entire PoP and shall permit timely development of all necessary cost data in the form required by the Contract.

### **H.12 APPROVED PURCHASING SYSTEM**

The objective of a contractor purchasing system assessment is to confirm it is a Government-approved purchasing system and evaluate the efficiency and effectiveness with which the contractor spends Government funds and complies with Government policy with subcontracting. A Government-audited and approved purchasing system (e.g., approved by DCAA or Defense Contract Management Agency (DCMA)) is not mandatory but is preferred.

When reviews are conducted of the purchasing system during the performance of the TO, the contractor shall provide the results of the review to the FEDSIM CO within ten workdays from the date the results are known to the contractor.

### **H.13 TRAVEL**

#### **H.13.1 TRAVEL REGULATIONS**

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

- a. FTR - prescribed by the GSA, for travel in the contiguous U.S.
- b. JTR, Volume 2, DoD Civilian Personnel, Appendix A - prescribed by the DoD, for travel in AK, HI, and outlying areas of the U.S.
- c. DSSR (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the DoS, for travel in areas not covered in the FTR or JTR.

As all contractor personnel are DoD-sponsored contractor personnel, the contractor shall ensure that all official and leisure travel complies with the requirements stipulated in the DoD Foreign Clearance Guide (FCG), host-country-specific requirements (e.g., BACO-90 ("Request for Confirmation of Exemption from the Requirement to Obtain a Work Permit") in Germany), and other applicable regulations.

#### **H.13.2 TRAVEL AUTHORIZATION REQUESTS (TAR)**

Before undertaking long-distance travel to any Government site or any other site in performance of this TO, the contractor shall have this long-distance travel approved by, and coordinated with, the FEDSIM COR. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long-

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

distance travel, the contractor shall prepare a TAR (**Section J, Attachment M**) for Government review and approval. Long-distance travel will be reimbursed for cost of travel comparable with the FTR or JTR and DSSR as applicable.

Requests for long-distance travel approval shall:

- a. Be prepared in a legible manner.
- b. Include a description of the travel proposed including a statement as to purpose.
- c. Be summarized by traveler.
- d. Identify the TO number.
- e. Identify the CLIN associated with the travel.
- f. Be submitted in advance of the travel with sufficient time to permit review and approval.
- g. Financial tracking data as necessary to meet USACE and FEDSIM cost tracking requirements (i.e., tracking at the division/site/project and or TDL level).

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Long-distance travel shall be scheduled during normal duty hours whenever possible.

### **H.13.3 OUTSIDE THE CONTINENTAL UNITED STATES (OCONUS) TRAVEL**

The contractor shall perform work at OCONUS locations and forward-deployed sites in combat zones or other high-threat areas. The contractor shall be required to prepare and obtain all necessary paperwork, documentation, and/or permits required for deployment. The website for Aircraft and Personnel Automated Clearance System (APACS) is <https://apacs.milcloud.mil/apacs/dtic.mil/apacs/>. The contractor shall obtain and maintain an account for access to the APACS site.

### **H.13.4 OUTSIDE THE CONTINENTAL UNITED STATES (OCONUS) DEPLOYMENT LOGISTICAL SUPPORT**

Logistic support by the Government will be provided within U.S.-occupied compounds.

### **H.13.5 FLAT RATE PER DIEM FOR LONG-TERM TEMPORARY DUTY (TDY)**

In order to encourage contractors to take advantage of cost saving opportunities available for long-term travel, contractors performing TDY for more than 30 days in one location (CONUS and OCONUS) will receive a flat rate per diem. The following rules apply:

- a. On the travel day to the TDY location, the contractor receives up to 100 percent lodging per diem at the locality rate, and 75 percent Meals and Incidental Expenses (M&IE).
- b. For long-term TDY lasting 31 -180 days (in a single location), the authorized flat rate is 75 percent of the locality rate (lodging plus M&IE) payable for each full day of TDY at that location.
- c. For long-term TDY of 181 days or greater (in a single location), the authorized flat rate is 55 percent of the locality rate (lodging plus M&IE) payable for each full day of TDY at

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

that location. Normally, TDY over 180 days will be prohibited, but may be authorized by the FEDSIM COR and FEDSIM CO when justified.

- d. When using a flat rate per diem, contractors are not required to submit a lodging receipt, but are required to validate to the USACE TPOC and FEDSIM COR that they did incur lodging costs.

If the contractor is unable to find suitable commercial lodging at the reduced per diem rate, it should contact the FEDSIM COR. If both the contractor and the FEDSIM COR determine that lodging is not available at the reduced per diem rate, the FEDSIM COR may then authorize actual cost lodging (not to exceed the locality per diem rate). However, the contractor will receive M&IE at the reduced rate (75 percent for TDY of 31-180 days and 55 percent for TDY of 181+ days).

### **H.13.6 DEFENSE BASE ACT (DBA) INSURANCE**

The contractor shall ensure that health and life insurance benefits provided to its deploying personnel are in effect in the theater of operations and allow traveling in military vehicles. Insurance is available under the DBA administered by the Department of Labor (DoL).

- a. Pursuant to FAR 28.305, DBA insurance coverage provides workers' compensation benefits (i.e., medical, disability, and death) in the event of a work-related injury or illness OCONUS.
- b. The Government requires that all contractor personnel who work internationally be protected by the DBA coverage, regardless of their assignment and/or location unless a waiver has been obtained by the DoL.

DBA insurance may be charged as a direct or indirect cost consistent with the contractor's CAS Disclosure Statement (D/S) and DCAA-approved accounting system, and shall be furnished to the FEDSIM CO within 30 days of TOA. If required and approved by the FEDSIM CO, additional DBA riders may be charged to the Government.

### **H.13.7 DEPLOYMENT REQUIREMENTS**

The requirements of this TO support the mission and operational readiness of the U.S. Armed Services operating worldwide.

The contractor shall ensure all contractor personnel participate in any required and/or necessary pre-deployment qualification training. The personnel in each team shall be available for deployment or duty at other designated CONUS locations at the end of that training period. USACE shall determine the actual initial deployment dates based on mission requirements. USACE will assess individual performance during training in order to validate readiness to perform all tasks and duties. The Government will provide the following training (as needed):

- a. Individual pre-deployment training in accordance with DoD and applicable Geographical Combatant Command requirements.
- b. Weapons qualification training, if required by arming authorization (only if authorized by the destination Theater Commander).

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

- c. Technical and functional training on regional operational procedures, the threat situation and all operational and intelligence tools necessary to perform duties when deployed with forward elements.

Contractor personnel will be integrated into Government contingency plans, and afforded the same rights, privileges, protection, and priority as U.S. Government personnel during execution of the contingency plan. The Government may provide security, housing, and messing facilities for contractor personnel should conditions warrant.

### **H.13.8 DEPLOYING CONTRACTOR PERSONNEL**

The CONUS Replacement Center (CRC) at Fort Bliss, TX (<https://home.army.mil/bliss/index.php/units-tenants/crc>) is currently the designated processing site for personnel deploying to Hazardous Duty (HD)/Combat Zone (CZ) locations. The FEDSIM CO or FEDSIM COR will notify the contractor in writing if the CRC location shall be other than Fort Bliss, TX. Contractor personnel being deployed to HD/CZ locations shall report to the designated CRC for pre-deployment processing. The CRC validates readiness and conducts deployment processing to the HD/CZ duty station. Deploying contractor personnel shall complete all pre-reporting requirements so they can deploy immediately upon completion of CRC processing. Pre-reporting requirements include, but are not limited to:

- a. Medical readiness.
- b. Theater-Specific Individual Readiness Training certifications.
- c. Current Individual Readiness File records needed for identification and processing.
- d. Valid passports and visas (for the longest period possible to mitigate a mid-tour break in service).
- e. Any other preparation to prevent rejection by the CRC.
- f. Contractor personnel determined by the CRC to be non-deployable will be referred back to the contractor for disposition.

The contractor may be issued personal/individual protection equipment when necessary and directed by the destination Theater Commander, in accordance with DoDI 3020.41 paragraph 3i.

### **H.13.9 PASSPORTS, VISAS, AND CUSTOMS**

The contractor shall be responsible for obtaining all passports, visas, or other documents necessary to enter and/or exit any area(s) identified by the FEDSIM COR for contractor personnel. The Government will reimburse the contractor for visa costs; however, the Government will not reimburse the contractor for any costs associated with obtaining passports.

All contractor personnel shall be subject to the customs processing procedures, laws, agreements, and duties of the country to which they are deploying and the procedures, laws, and duties of the U.S. upon re-entry.

The contractor shall register all personnel with the appropriate U.S. Embassy or Consulate where possible.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

### **H.13.10 CONTRACTOR COMPLIANCE**

The contractor shall ensure that all contractor and subcontractor personnel comply with all guidance, instructions, and general orders applicable to U.S. Armed Forces and DoD civilians and issued by the Theater Commander or his/her representative. This shall include any and all guidance and instructions issued based upon the need to ensure mission accomplishment, force protection, and safety.

The contractor shall comply, and ensure that all deployed personnel comply, with pertinent Service and DoD directives, policies, and procedures. The contractor shall ensure compliance with all Federal statutes, judicial interpretations, and international agreements (e.g., SOFAs, Host Nation Support Agreements, etc.) applicable to U.S. Armed Forces or U.S. citizens in the area of operations. The FEDSIM CO will resolve disputes. Host Nation laws and existing SOFAs may take precedence over TO requirements.

- a. The contractor shall take actions to ensure the professional conduct of its personnel and subcontractors.
- b. The contractor shall promptly resolve, to the satisfaction of the FEDSIM CO, all contractor personnel performance and conduct problems identified by the USACE TPOC, FEDSIM CO, or FEDSIM COR.
- c. The FEDSIM CO may require the contractor, at the contractor's expense, to remove or replace any individual failing to adhere to instructions and general orders issued by the Theater Commander or his/her designated representative.

### **H.13.11 SPECIAL LEGAL CONSIDERATIONS**

**Public Law 106-523 - Military Extraterritorial Jurisdiction Act of 2000:** Amended Title 18, U.S.C., establishes Federal Jurisdiction over certain criminal offenses committed outside the U.S. by persons employed by or accompanying the Armed Forces, or by members of the Armed Forces who are released or separated from active duty prior to being identified and prosecuted for the commission of such offenses, and for other purposes.

**Applicability:** This Act applies to anyone who engages in conduct outside the U.S. that would constitute an offense punishable by imprisonment for more than one year, the same as if the offense had been committed within the jurisdiction of the U.S. The person must be employed by or accompanying the Armed Forces outside the U.S.

### **H.13.12 ACCOUNTING FOR PERSONNEL**

As required by the USACE TPOC, FEDSIM CO, or FEDSIM COR and based on instructions of the Theater Commander, the contractor shall report its employees, including Third-Country Nationals (TCNs), entering and/or leaving the area of operations by name, citizenship, location, Social Security Number (SSN), or other official identity document number.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

### **H.13.13 THEATER RISK ASSESSMENT AND MITIGATION**

If a contractor individual departs an area of operations without contractor permission, the contractor shall ensure continued performance in accordance with the terms and conditions of the TO. If the contractor replaces an individual who departs without permission, the replacement is at contractor expense and must be in place within 30 Calendar days or as instructed by the FEDSIM CO.

For badging and access purposes, the contractor shall provide the USACE TPOC and FEDSIM COR a list of all personnel (this includes subcontractors and/or local vendors being used in the area of operations) with the required identification and documentation information.

The contractor shall brief its employees regarding the potential danger, stress, physical hardships, and field living conditions.

The contractor shall require all of its employees to acknowledge in writing that they understand the danger, stress, physical hardships, and field living conditions that are possible if the employee deploys in support of military operations.

The contractor shall designate a POC for all of its plans and operations and establish an operations center to plan and control the contractor deployment process and resolve operational issues with the deployed force.

### **H.13.14 FORCE PROTECTION**

While performing duties in accordance with the terms and conditions of the TO, the Service/Agency (e.g., Army, Navy, Air Force, Marine, Defense Logistics Agency (DLA)) will provide force protection to contractor employees commensurate with that given to Service/Agency civilians in the operations area. Contractor employees should be made aware of force protection provided by the Government and NOT take any actions that would put themselves in harm's way beyond what is reasonable and expected from the conditions offered by the services.

### **H.13.15 EMERGENCY LEAVE**

In OCONUS areas, emergency leave travel is chargeable to this TO. If a contractor employee is in a deployment location and an emergency occurs, the Government will normally accommodate the emergency leave once the emergency is verified by the Red Cross. If the contractor has questions on what constitutes emergency leave, the contractor shall refer to DoDI 1327.06 dated June 2009.

If a contractor individual departs an area of operations for an emergency leave, the contractor shall ensure continued performance in accordance with the terms and conditions of the TO or as instructed by the FEDSIM CO. If the contractor replaces an individual who departs for an emergency leave, the replacement personnel shall be in place within 14 Calendar days or as instructed by the FEDSIM CO.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

### **H.13.16 LIVING UNDER FIELD CONDITIONS**

If requested by the contractor, and if available, the Government will provide contractor employees deployed in the theater of operations the equivalent field living conditions, subsistence, emergency medical and dental care, sanitary facilities, mail delivery, laundry service, and other available support afforded to Government employees and military personnel in the theater of operations.

### **H.13.17 MORALE, WELFARE, AND RECREATION (MWR)**

The Government will provide contractor employees deployed in the theater of operations MWR services commensurate with that provided to DoD civilians and military personnel deployed in the theater of operations.

### **H.13.18 NEXT OF KIN NOTIFICATION**

Before deployment, the contractor shall ensure that each contractor employee completes a DD Form 93, Record of Emergency Data Card, and returns the completed form to the designated Government official. The contractor shall be responsible for establishing a line of communication to notify and inform its employees' families of the status of the employee while he/she is deployed. The Government will be responsible for ensuring that the contractor is notified of its employees' status at the earliest possible time without compromising national security. The Government reserves the right to notify families of contractor employees' status only when it is in the best interest of the Government.

### **H.13.19 RETURN PROCEDURES**

Upon completion of the contractor's tour, contractor personnel shall redeploy and out-process through the CRC in accordance with DoDI 3020.41. The contractor shall enforce this requirement and refrain from allowing the contractor employee to bypass the CRC for out-processing. The deployment site/center that prepared the contractor for deployment will serve as the return processing center.

Upon notification of return, the USACE TPOC may authorize and the FEDSIM COR may approve contractor employee travel from the theater of operations to the designated individual deployment site. The contractor shall ensure that all GFP provided to the contractor or the contractor's employees are returned to Government control upon completion of the deployment. The contractor shall provide the USACE TPOC and FEDSIM COR with documentation, annotated by the receiving Government official, of all equipment returns. The contractor shall be liable for any GFP not returned to the Government.

### **H.13.20 HARDSHIP AND DANGER PAY**

Post (Hardship) Differential and Danger (Hazard) pay are allowances that provide additional compensation above basic compensation in a foreign area as determined by the DoS where civil insurrection, civil war, terrorism, or wartime conditions threaten physical harm or imminent danger to the health or well-being of the employee. The contractor shall be reimbursed for



## SECTION H – SPECIAL CONTRACT REQUIREMENTS

payments made to its employees for danger pay, not to exceed that paid U.S. Government civilian employees, in accordance with the provisions of the DSSR Chapter 500 – Post (Hardship) Differential, Chapter 650 - Danger Pay Allowance, and Section 920 - Post Classification and Payment Tables, as may be amended. Compensation to “Basic Compensation” shall be only applicable to the first 40 hours of effort performed per week. Hardship and danger pay shall be billed as an ODC.

### **H.13.21 SECURE HOUSING SUPPORT**

The contractor shall acknowledge at least 10 workdays before travel (unless given less notice for travel by the Government, then within one workday from travel notice) that it is prepared, if required by the Government, to house and sustain, including feeding, its personnel in deployment locations and to accept/establish a secure housing facility off of the U.S. compound. The USACE TPOC or FEDSIM COR will provide the contractor with written notification if the contractor must billet its personnel outside of the U.S. compound. Security and other services for the secure housing facility (including transportation to and from assigned duty location, if the duty location is on a U.S. or Coalition Force compound) may be provided by using TCN and Local National staff, subcontracted for by the contractor awarded this TO. Security service providers shall be on the approved vendor listing of both U.S. Forces and the Host Nation Government. All costs associated with this support, if implemented, shall be billed to the TO as an ODC. Secure housing facility support staff, including security staff, will not be sponsored (issued a CAC and/or a Letter of Authorization (LOA)) by the Government under this TO. Construction is prohibited.

### **H.13.22 SYNCHRONIZED PRE-DEPLOYMENT AND OPERATIONAL TRACKER (SPOT)**

The SPOT system is used to generate LOAs which define specific Government services and support all contractor personnel who are authorized to work in a deployment area. The contractor shall process LOAs in SPOT for all contractor personnel deploying under the TO and the additional documentation required with each LOA. The contractor shall fully execute all SPOT requirements.

### **H.13.23 STATUS OF FORCES AGREEMENTS (SOFAs)**

In consultation with the servicing legal advisor, the USACE TPOC will inform the contractor of the existence of all relevant SOFAs (**Section J, Attachment P**) and other similar documents, and provide copies upon request. The contractor shall be responsible for obtaining all necessary legal advice concerning the content, meaning, application, etc. of any applicable SOFAs, and similar agreements. The contractor shall adhere to all relevant provisions of the applicable SOFAs and other similar related agreements.

Invited Contractor and Technical Representative (TR) status shall be governed by the various SOFAs implemented by U.S. Forces in a variety of theaters (e.g., South Korea, Italy, and Germany). The contractor shall coordinate with the Government to satisfy all requirements by

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

the governing regulations for the specified theater. The contractor shall do the initial research into the requirements and inform the Government as to what the requirements are to travel into theater. It is agreed that the withdrawal of Invited Contractor or TR status, or the withdrawal of or failure to provide any of the privileges associated therewith by the U.S., shall not constitute grounds for excusable delay by the contractor in the performance of the TO and will not justify or excuse the contractor defaulting in the performance of this TO. Furthermore, withdrawal of SOFA status for any reason shall not serve as a basis for the contractor filing any claims against the U.S.

### **H.13.23 OUTSIDE THE CONTINENTAL UNITED STATES (OCONUS) TRAVEL**

The contractor shall perform work at OCONUS locations and forward-deployed sites in combat zones or other high-threat areas. Contractor personnel shall require an APACS Theater/Country clearance for travel to OCONUS locations. The contractor shall be required to prepare and obtain all necessary paperwork, documentation, and/or permits required for deployment. The website for APACS is <https://apacs.milcloud.mil/apacs/dtic.mil/apacs/>. The contractor shall obtain and maintain an account for access to the APACS site.

### **H.13.24 RELOCATION AND REPATRIATION**

The Government will reimburse the contractor for reasonable and allowable costs, as determined by the FEDSIM CO and FEDSIM COR, associated with relocating and repatriating personnel from/to the individual's CONUS home of record to/from the assigned OCONUS performance location, excluding HI and AK. In determining what is considered reasonable and allowable, the Government will consider FAR 31.205-35 and what is afforded to U.S. Government civilian employees under the JTR.

If the Government does not reimburse the contractor for an individual's relocation expenses (e.g., the individual was a local hire), in order for that individual to be eligible for Government reimbursement of repatriation costs, that individual shall commit to a minimum 24-month service commitment or until the end of the TO if there are less than 24 months of performance left, which commences when the individual begins work under this TO in the assigned position. If the individual vacates the position without Government direction prior to the 24-month mark or the end of the TO if there are less than 24 months of performance left, the contractor shall bear all costs to repatriate the individual.

If the Government reimburses the contractor for an individual's relocation expenses, that individual shall commit to a minimum 24-month service commitment or until the end of the TO if there are less than 24 months of performance left, which commences when the individual arrives at the designated place of performance and begins work, under this TO and in the place of performance that the individual was relocated to at Government expense. If that individual vacates the position and/or place of performance without Government direction prior to the 24-month mark or the end of the TO if there are less than 24 months of performance left, the contractor shall bear all costs associated with repatriating the individual and all costs associated with relocating a new individual to fill the position.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

The Government will consider exceptions to the relocation and repatriation policy on a case-by-case basis. The contractor shall address all requested exceptions with the FEDSIM COR and the final decision will be made by the FEDSIM CO and FEDSIM COR.

The contractor shall develop an SOP (**Section F, Deliverable 61**) that outlines in detail the contractor's processes and procedures for managing relocation and repatriation activities and the contractor's proposed relocation and repatriation costs. This SOP shall be submitted to the Government as part of the contractor's PMP. The contractor shall operate in accordance with the most recent Government-approved version of the SOP/PMP.

Prior to incurring any costs associated with the relocation and/or repatriation of personnel that the contractor intends to charge to the Government, the contractor shall submit an RIP that identifies the specific charges and estimated associated costs for the FEDSIM COR's review and approval.

Travel-related expenses associated with the relocation and/or repatriation of personnel shall be submitted in a TAR and charged under the travel CLIN. This includes, but is not limited to, airfare, lodging, and per diem expenses incurred prior to the individual obtaining housing and becoming eligible for LQA in accordance with Section H.13.26.1. The Government will reimburse the contractor for lodging and per diem costs associated with relocation and/or repatriation for up to 60 days and will utilize the flat rate per diem model, detailed in Section H.13.26.3, at the 31- to 180-day rate regardless of how long the contractor occupies temporary housing. Reimbursement for lodging and per diem expenses incurred prior to the individual obtaining housing and associated with the relocation and/or repatriation of personnel will be for one individual only, regardless of family size.

### **H.13.25 OUTSIDE THE CONTINENTAL UNITED STATES (OCONUS) ALLOWANCES**

The Government will reimburse the contractor for the allowances and benefits identified in Section H. If an allowance or benefit is not specifically identified in the TO and the contractor would like the Government to consider allowing for reimbursement, then the contractor may submit a request in writing to the FEDSIM CO and FEDSIM COR that contains, at a minimum, a summary of the request, a justification for why it is in the Government's best interest, and the associated estimated cost(s). Final decisions will be made by the FEDSIM CO and FEDSIM COR, and if necessary, the TO will be amended by a bilateral modification.

#### **H.13.25.1 QUARTERS ALLOWANCE**

Chapter 100 of the DSSR outlines quarters' allowances, which include:

- a. Temporary quarters' subsistence allowance.
- b. LQA.
- c. Extraordinary quarters' allowance.

Under this TO, the Government will reimburse the contractor for LQA expenses only (item b. above), in accordance with DSSR Section 130 – Living Quarters Allowance. The Government

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

will not reimburse the contractor for any other quarters allowances identified in the DSSR which includes items a. and c. above. LQA will be reimbursed in accordance with the provisions of DSSR Section 130 – Living Quarters Allowance and at the rates established by the DSSR specific to each foreign location.

DSSR Section 136 – Personally Owned Quarters and DSSR Section 137 – Allowance for Necessary and Reasonable Initial Repairs, Alterations, and Improvements Under Unusual Circumstances are not applicable to this TO.

The contractor shall develop an SOP (**Section F, Deliverable 62**) that outlines in detail the contractor's processes and procedures for managing LQA. At a minimum, the SOP shall address the Government requirements identified in the TO and roles and responsibilities. This SOP shall be submitted to the Government as a part of the contractor's PMP. The contractor shall operate in accordance with the most recent Government-approved version of the SOP/PMP.

As stated in DSSR Section 131.1, the purpose of LQA is to reimburse the contractor for the annual cost of suitable, adequate, living quarters for the employee and his/her family. The rates established by the DSSR specific to each foreign location represent the maximum amount that may be reimbursed by the Government in a 12-month period for an individual. The DSSR updates these rates on a biweekly basis throughout the year. Key Personnel and additional proposed Key Personnel identified in Section H.1 of the TO are eligible for reimbursement at the Quarters Group 2 rate. All other contractor personnel, determined by the FEDSIM COR to be eligible for LQA reimbursement, will be reimbursed at the Quarters Group 3 rate. The Government will not reimburse any expenses and/or costs that exceed the DSSR-specified maximum amount.

Contractor personnel are not eligible for LQA reimbursement from the Government until approved by the FEDSIM COR. Prior to incurring any LQA costs that the contractor intends to charge to the Government, the contractor shall submit an RIP to the FEDSIM COR that includes, at a minimum, the employee name, location, quarters group, OASIS labor category, family size, the current DSSR-specified maximum amount per year, and the requested monthly LQA amount based on the projected actual costs. Once the RIP has been approved by the FEDSIM COR, the contractor is permitted to invoice at the approved monthly amount. Once the RIP has been approved, if the contractor would like to change the monthly amount for an employee(s), the contractor shall submit a new RIP that contains a justification for the change.

The LQA amounts reimbursed by the Government to the contractor shall not in any circumstances exceed the actual costs paid by the contractor. As a result, the contractor shall conduct an Annual LQA Reconciliation (**Section F, Deliverable 63**) to determine:

- a. The maximum LQA amount that each contractor employee was eligible to receive in accordance with the rates established by the DSSR specific to each foreign location (taking into account the biweekly fluctuations that occur).
- b. The actual costs incurred by each contractor employee.
- c. The amount of LQA that each contractor employee received from the Government.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

The annual reconciliation shall be completed for all contractor employees who received LQA during the applicable TO PoP. In the annual reconciliation, the contractor shall determine if the Government either over- or under-paid any contractor employees. The contractor shall also determine if any adjustments to current LQA amounts, due to either gross over- or under-payment, are necessary, and if so, the contractor shall submit new RIP(s) within seven workdays.

Once the FEDSIM COR has accepted the Annual LQA Reconciliation in accordance with Section E, the contractor may submit an invoice to the Government for any additional LQA owed. If the contractor owes the Government a credit due to over-payments, the contractor shall provide that credit within 30 calendar days of the FEDSIM COR's acceptance of the annual reconciliation. The Government reserves the right to request backup documentation from the contractor in the form of leases, utility bills, etc. in order to verify the information presented by the contractor in the annual reconciliation.

Utility Tax Avoidance Program (UTAP) - The finance ministries of the NATO Forces established the UTAP to allow authorized customers tax-free utilities with participating utility companies. The UTAP is designed for service members assigned to Europe, U.S. civilians working for the U.S. Forces, and accredited contractors (Articles 72 & 73, TESA/ASSA Approval). Beginning in February 2012, DoD mandated use of UTAP for all LQA recipients in an effort to secure effective tax relief from foreign taxes on residential consumption of electricity, gas, and water in Germany. To be eligible for UTAP individuals must receive their utilities from a provider that has a contractual agreement with the U.S. Army Garrison Tax Relief Office (TRO). Some utilities could fall under additional cost "Nebenkosten," paid directly to the landlord, these costs are not covered by UTAP. UTAP requires a non-reimbursable \$99 registration fee per residence.

### **H.13.25.2 COST OF LIVING ALLOWANCE (COLA)**

Chapter 200 of the DSSR outlines COLA which include:

- a. Post Allowance
- b. Foreign Transfer Allowance
- c. Home Service Transfer Allowance
- d. Separate Maintenance Allowance
- e. Education Allowance
- f. Educational Travel

The Government will reimburse the contractor for education expenses only (item e. above), in accordance with DSSR Section 270 – Education Allowance, under this TO. The Government will not reimburse the contractor for any other COLAs identified in the DSSR which includes items a. through d. and f. above.

Education allowances will be reimbursed in accordance with the provisions of DSSR Section 270 – Education Allowance and at the rates established by the DSSR specific to each foreign location. Prior to incurring any education costs that the contractor intends to charge to the

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

Government, the contractor shall submit an RIP for each school year that lists by employee name and location, the requested education allowance(s), and associated school grade for each child.

The rates established by the DSSR specific to each foreign location represent the maximum amount that may be reimbursed by the Government. The contractor shall invoice the Government based on the actual costs incurred up to the maximum amount authorized by the DSSR specific to each foreign location.

### **H.13.25.3 HOME LEAVE**

The Government will not reimburse the contractor for home leave under this TO.

### **H.14 TOOLS (HARDWARE/SOFTWARE) AND/OR ODCs**

The Government may require the contractor to purchase hardware, software, and related supplies critical and related to the services being acquired under the TO. Such requirements will be identified at the time a TOR is issued or may be identified during the course of a TO by the Government or the contractor. If the contractor initiates a purchase within the scope of this TO, the contractor shall submit to the FEDSIM COR an RIP (**Section J, Attachment N**). If the prime contractor is to lose an approved purchasing system, the contractor shall submit to the FEDSIM CO a CTP (**Section J, Attachment O**). The RIP and CTP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. The contractor shall not make any purchases without an approved RIP from the FEDSIM COR or an approved CTP from the FEDSIM CO and without complying with the requirements of Section H.17 Commercial Supplier Agreements.

### **H.15 TECHNICAL DIRECTION LETTERS (TDLs)**

TDLs are a means of communication between the FEDSIM COR, USACE TPOC, and the contractor to answer technical questions, provide technical clarification, and give technical direction regarding the content of the PWS (see Section C). Technical direction means clarification of contractual requirements or direction of a technical nature, within the context of the PWS of the contract. In this capacity, the FEDSIM COR and USACE TPOC may provide technical direction to the contractor, so long as the technical direction does not make any commitment or change that affects price, quality, quantity, delivery, or other terms and conditions of the contract. However, only the FEDSIM CO may authorize the implementation of the TDL, and the FEDSIM COR and USACE TPOC work within the limitations of the TDL. Once the FEDSIM CO authorizes work via a TDL, the contractor shall prepare a TDP in accordance with Section C.5.1.15. When necessary, the FEDSIM CO, in coordination with the FEDSIM COR and USACE TPOC, will provide the contractor with TDLs concerning details set forth in this TO subject to the following limitations:

- a. The TDL must be in writing and be concurred to by the USACE TPOC and the FEDSIM COR and approved by the FEDSIM CO prior to issuance of the TDL to the contractor. Any subsequent amendments to the TDL must be in writing and be concurred to by the USACE TPOC and FEDSIM COR, and approved by the FEDSIM CO prior to issuance

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

of the TDL to the contractor. Written TDLs are the only medium permitted for use when technical direction communication is required. Any other means of communication (including, but not limited to, the Contractor Service Request Letters, Authorization Letters, or Material Budget Letters) are not permissible means of communicating technical direction during Contract performance.

- b. Each TDL issued is subject to the terms and conditions of this TO and will not be used to assign new work, direct a change to the quality or quantity of supplies or services delivered, change the delivery date(s) or PoP of the contract, or change any other conditions of the contract. TDLs will only provide additional clarification and direction regarding technical issues. In the event of a conflict between a TDL and the TO, the TO will take precedence.
- c. Issuance of TDLs will not incur an increase or decrease to the Contract price, estimated Contract amount (including fee), or Contract funding, as applicable. Additionally, TDLs will not provide clarification or direction of a technical nature that would require the use of existing funds on the Contract beyond the PoP or delivery date for which the funds were obligated.
- d. TDLs will provide specific technical direction to the contractor only for work specified in the PWS and previously negotiated in the TOR. TDLs will not require new TO deliverables that may cause the contractor to incur additional costs. Each TDL will identify what tasks under Section C apply and provide instructions for each task to the contractor.
- e. When, in the opinion of the contractor, a TDL calls for effort outside the terms and conditions of the Contract or available funding, the contractor shall notify the FEDSIM CO in writing, with a copy to the FEDSIM COR, within two working days of having received the technical direction. The contractor shall undertake no performance to comply with the TDL until the matter has been resolved by the FEDSIM CO through a contract modification or other appropriate action.

When necessary, technical direction concerning the details of specific tasks set forth in the TO shall be given through issuance of TDLs by the FEDSIM CO. The Government will notify the contractor of the need to issue an approved TDL to the contractor (signed by FEDSIM CO, FEDSIM COR, USACE TPOC, and contractor), and a resulting TO funding modification when required.

### **H.16 SYSTEMS, CERTIFICATIONS, AND CLEARANCES**

All contractor employees working cybersecurity/IT functions must comply with DoD and Army training requirements in DoD Directive (DoDD) 8140, DoD 8570.01-M, and AR 25-2 upon Contract award.

Per DoD 8570.01-M, DFARS 252.239.7001 and AR 25-2, the contractor employees supporting IA/IT functions shall be appropriately certified upon Contract award. The baseline certification as stipulated in DoD 8570.01-M shall be completed upon Contract award.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

Contractor personnel shall meet and maintain the background investigation and adjudication requirements called for in DoD 5200.2-R, the DoD Personnel Security Program for the IT level designation for their position as defined in the duty appointment. Foreign National (FN) personnel may not be assigned to IT Level –I positions. For positions identified as IT-II and IT-III, FNs may be appointed if they possess a unique or unusual skill or expertise that is urgently needed for a specific DoD requirement and for which a suitable U.S. citizen is not available, and approved in writing by the COR. However, under no circumstances can these individuals be assigned before completion and favorable adjudication of the appropriate security background investigation. USACE retains the right to request removal of contractor personnel, regardless of prior clearance or adjudication status, whose actions while assigned to this Contract are determined to be detrimental to the overall performance of the Contract or the best interests of the Government as determined by the FEDSIM CO. The reason for the request for removal will be fully documented in writing by the FEDSIM COR and submitted through the FEDSIM CO for approval and issuance to the contractor.

Contractor employees accessing the Government network are required to be citizens of the U.S. and must maintain that status for the duration of the Contract.

Contractor employees accessing the Government network must meet security clearance requirements for performance and Government facility access.

The contractor shall submit verification of this check for each employee accessing the Government network on the task to the ERDC Security Office prior to the employee beginning work. If required, the ERDC Security Office, or other designated Government POC, will provide DD254 for contractor completion at time of award.

Common Access Card (CAC). The Government will provide special access badges as necessary. The Prime Contractor Facility Security Officer (FSO) shall ensure that all contractor personnel acquire and maintain CACs. The approving Government Trusted Agent (TA) may give access to the FSO using the online Trusted Associate Sponsorship System (TASS), <https://www.dmdc.osd.mil/tass>. Contractor eligibility remains in force during employment under the Contract for those employees who have a valid and recurring requirement for access to Government facilities or automation systems (reference DD254 for additional security requirements) to perform those duties stipulated in the Contract. The contractor shall use a valid CAC to access the Government domain. The contractor shall immediately return the CACs to the FEDSIM COR or USACE TPOC when the contractor employee's employment is terminated or upon expiration of the Contract. The CACs will expire when contractor employee eligibility terminates or three years from the issuance date, whichever occurs first. The contractor is responsible for all CACs and shall report all lost or stolen CACs to the FEDSIM COR immediately.

Subcontractor employees shall be considered contractor employees for the purpose of security requirements.

All network account access, user and administrative, shall be requested via the formal account request process and must be approved by the Government service owner, the personnel security



## SECTION H – SPECIAL CONTRACT REQUIREMENTS

manager, and an Information System Security Officer or Manager who will validate need to access/know, personnel security requirements, and cybersecurity workforce standards are met prior to account issuance.

All contractor employees and associated subcontractor employees shall complete the DoD Cyber Awareness Challenge training and sign the acceptable use policy before issuance of network access and annually thereafter. All contractor employees working Cybersecurity (CS)/IA/IT functions shall be fully baseline (and computing environment only for positions as required by policy) certified prior to engagement and must comply with requirements in accordance with DoD 8570.01M Information Assurance Workforce Improvement Program, AR 25-2, DA PAM 25-2-6, DoD Directive 8140.01 Cyberspace Workforce Management, DoD Directive 5220.6 Defense Industrial Personnel Security Clearance Review Program, and DoD Manual 5205.02 DoD Operations Security (OPSEC) Program Manual which establish Cyber Workforce Qualification regulatory requirements, policy, procedures, and IA training levels for the IA/cyber workforce, which includes contractor personnel. USACE's Information Assurance Workforce Security Standards, Documentation, Training and Certification Memorandum and USACE's Information Assurance Workforce Security Standards Computing Environment Requirement for Specific Designated Roles further detail requirements specific to the USACE environments.

Contractor performing IA/cyber functions on DoD systems must meet the requirements established for the category and level function in which they are performing. Contractors assigned to cyber duties or with an IA designation as defined in policy will possess all qualification requirements as defined in the references above. Privileged access for all IA-designated roles will not be approved until such requirements have been met. Qualification requirements include, but are not limited to, initial training, IA Baseline Certification, On-the-job training evaluation, Computing Environment (CE) training or certification (as defined by the level designated), continuous education (required for computing environment and by baseline or computing environment certification service provider stipulations), required years of experience, required background investigation, and the Acceptable Use Policy, Privileged Access Agreement and an NDA have been signed, and Duty Appointment Letter has been authorized. All required documentation, training, and certification shall be recorded in ATCTS and verified by an ATCTS administrator to be considered valid.

### **H.17 COMMERCIAL SUPPLIER AGREEMENTS**

**H.17.1** The Government understands that commercial software tools that may be purchased in furtherance of this TO, as described in **Section C** and as contemplated in the Tools or ODC CLIN in **Section B**, may be subject to commercial agreements which may take a variety of forms, including without limitation licensing agreements, terms of service, maintenance agreements, and the like, whether existing in hard copy or in an electronic or online format such as “clickwrap” or “browsewrap” (collectively, “Supplier Agreements”). The contractor shall provide all applicable supplier agreements to the FEDSIM CO prior to purchase and shall cooperate with the Government in negotiating suitable terms to comply with this Section which shall be “specific rights” pursuant to DFARS 227.7202-3.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

**H.17.2** Commercial computer software or commercial computer software documentation shall be acquired under the licenses customarily provided to the public unless such licenses are inconsistent with Federal procurement law or do not otherwise satisfy the objectives of this TO. Notwithstanding any contrary provisions contained in the contractor's standard commercial license or lease agreement, the contractor agrees that the Government will have the rights that are set forth in paragraph (b) of DFARS 227.7202-3 to use, duplicate, or disclose any commercial computer software delivered under this TO.

### **H.18 PRESS/NEWS RELEASE**

The contractor shall not make any press/news release pertaining to this procurement without prior Government approval and only in coordination with the FEDSIM CO.

Release of any information on this Contract to any person or organization who is not a party to this Contract is prohibited without the prior written permission of USACE. This information includes proprietary information, news stories, articles, sales literature, TV-radio spots, advertisements, etc. All requests for review/public release will be forwarded to the USACE TPOC, FEDSIM COR, and FEDSIM CO.

### **H.19 CONTRACTOR IDENTIFICATION**

The contractor shall advise and assist the Government, but it shall neither make final decisions or certifications on behalf of the Government nor perform any inherently governmental functions per FAR 7.503. The contractor or its employees shall neither represent the Government nor appear to represent the Government in performance of these contract services. As stated in 48 CFR 211.106, Purchase Descriptions for Service Contracts, contractor personnel shall identify themselves as contractor personnel by introducing themselves or being introduced as contractor personnel and by displaying distinguishing badges or other visible identification for meetings with Government personnel. Contractor personnel shall appropriately identify themselves as contractor employees in telephone conversations and in formal and informal written correspondence.

Contractor personnel performing services on DoD installations or other Government facilities shall ensure that they are readily identifiable as contractor employees. The contractor shall contact the USACE Government requiring activity to obtain the necessary base entry procedures.

Contractor employees without access to a DoD or other Government LAN systems shall:

- a. Identify themselves as contractor personnel at the onset of every telephone call made from a Government telephone or any other phone if the call is made in support of any service provision to the Government.
- b. Identify themselves as contractor personnel in all recorded messages, including those which are heard by callers attempting to contact contractor employees via answering machines or voicemail.
- c. Identify themselves as contractor personnel at the onset of every meeting, conference, or any other gathering attended in support of any service provision to the Government.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

- d. Identify themselves as contractor personnel on any correspondence, documents, or reports accomplished or sent in support of any service provision to the Government, including, but not limited to, correspondence sent via the U.S. mail, facsimile, or email inclusive of “out-of-office” replies.
- e. Wear or display contractor-provided nametags, badges, or attire which display, at a minimum, the name of the contractor.
- f. Any work under this Contract which is performed by the contractor or any of its subcontractors on premises under Government control is subject to all requirements of this Contract governing such work, and the following:
  - 1. All contractor and subcontractor personnel shall, at all times, conspicuously display a distinctive badge provided by the contractor, identifying such personnel as employees of the contractor, and shall observe and otherwise be subject to such security regulations as are in effect for the particular premises involved.
  - 2. All contractor and subcontractor personnel shall be easily recognized by wearing Government-provided security badges while working in a U.S. Government facility.
  - 3. The contractor shall designate in writing, an on-the-premises representative to serve as the POC for the contractor to the FEDSIM CO or their duly authorized representative.

All contractor and subcontractor employees shall dress appropriately for a professional work environment.

### **H.20 EXTENDED WORKWEEK**

The contractor shall define its work period/pay period to the USACE TPOC and FEDSIM COR. The contractor shall obtain written approval from the FEDSIM COR and FEDSIM CO prior to incurring any billable extended hours in excess of the contractor work period/pay period. Any services that extends beyond the contractor work period/pay period are considered extended and shall be billed at non-premium rates. When requesting written approval from the Government, an explanation for the anticipated extended workweek shall be included. Approval of such requests applies only to the individual(s) named in the request and is not transferable to others.

Written approval from the USACE TPOC and FEDSIM COR shall be obtained the month prior to the extended work period/pay period occurrence. The contractor shall have until the last day of each work period/pay period to obtain approval of an extended period for the upcoming month. In the event of an unanticipated extended work period/pay period, the contractor shall obtain approval NLT Thursday of the week in which the extended period will occur.

An extended work period/pay period may occur at a place of performance listed in Section F.2 or a TDY station assignment either CONUS or OCONUS.

### **H.21 FACILITY CLOSINGS**

During a normal workweek, if any Federal facility listed as a place of performance in Section F is closed, opens late, or closes early, due to Government Federal Holidays, inclement weather

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

(e.g., ice, snow, etc.), or other special circumstances, duty time for contractor personnel scheduled to work at the facility shall not constitute as billable time unless upon Government approval. The contractor shall not include any hours for which the on-site facilities are not available for performance.

The FEDSIM COR and USACE TPOC may authorize the contractors to work at an off-site location while Government facilities are closed. The FEDSIM COR, in conjunction with the USACE TPOC, will allow contractor employees to adjust their schedules to compensate for missed times and have the option to work extended workdays, if desired.

### **H.22 CONTRACTOR-PROVIDED FACILITIES**

The contractor shall secure and maintain assigned facilities or provide alternate facilities when no Government facilities are available.

Work covered under this task does not include the acquisition of land or the erection of permanent facilities.

All leasing requirements specified in the Alliant 2 basic contract apply to this TO. If leasing occurs under this TO, the Government will not be the Lessee. Prior to entering into ANY leasing agreement, the contractor shall coordinate with the FEDSIM COR and USACE TPOC and have an approved RIP from the FEDSIM COR. Under no circumstances will the Government be deemed to have privity of contract with the Owner/Lessor of the leased items; nor will the Government be held liable for early termination/cancellation damages if the Government decides not to exercise an option period under a TO.

#### **H.22.1 CONTINENTAL UNITED STATES (CONUS) SUPPORT FACILITIES**

The contractor shall provide CONUS support facilities as required by the Government. Requirements for additional CONUS support facilities will be identified by TDL specifying the facility's purpose, locations, and required space.

#### **H.22.2 INFORMATION SECURITY OPERATIONS CONTRACTOR FACILITY**

The contractor shall provide facilities necessary to support SOC/NOC/service desk support in CONUS locations, including providing necessary redundancies. The contractor-provided NOC/SOC capability shall be in accordance with DoDI 8530.01.

### **H.23 INTELLECTUAL PROPERTY RIGHTS**

The existence of any patent, patent application or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, the data rights provisions in DFARS 252.227-7013 and 252.227-7014 or FAR 52.227-14 applies. The contractor shall provide the Government Unlimited Rights to the TO deliverables, as indicated in Section F.3 where DFARS 252.227-7013 and 252.227-7014 apply.

## SECTION H – SPECIAL CONTRACT REQUIREMENTS

### **H.24 ACCIDENT PREVENTION PLAN**

The Contractor shall prepare an Accident Prevention Plan in accordance with EM 385-1-1. The plan shall be prepared prior to the start of work and submitted as part of the contractor's PMP (**Section F, Deliverable 13**)

The Contractor shall prepare and submit an accident report using ENG Form 3394, if an accident occurs to a contractor or sub contractor employee while working on elements of this contract and maintain an accurate record of the accident if it results in traumatic injury, occupational illness, death or damage to government property in excess of \$2,000.00 in accordance with EM 385-1-1 77165-77170).

All accidents meeting the reporting requirements according to EM 385-1-1 for contractor or sub contractors will be investigated and reported to the COR and TPOC. The contractor will report accidents meeting the reporting requirements to the COR and TPOC no later than 24 hours after occurrence.

The APP or the USACE project safety and health plan shall provide for frequent safety inspections/audits, conducted by a Competent Person, of the work sites, material, and equipment to ensure compliance with the APP and EM 385-1-1. These inspections/audits shall be documented in writing and available upon request to the COR and TPOC. They shall include the name of the inspector, date and all findings. Records will be maintained providing factual evidence that QC activities for safety have been performed (i.e., job safety evaluations state what was checked, results, and instructions or corrective actions).

## SECTION I – CONTRACT CLAUSES

### **I.1 TASK ORDER CLAUSES**

All applicable and required clauses set forth in FAR 52.301 automatically flow down to all Alliant 2 TOs, based on their specific contract type (e.g., cost, fixed-price, etc.), statement of work, competition requirements, commercial or not commercial, and dollar value as of the date the TO solicitation is issued.

### **I.2 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)**

This TO incorporates one or more clauses by reference with the same force and effect as if they were given in full text. Upon request, the FEDSIM CO will make their full text available. Also, the full text of a clause may be accessed electronically at the FAR website:

<http://www.acquisition.gov/far/>

FAR Part 12 commercial clauses do not apply to this TO.

<b>FAR</b>	<b>TITLE</b>	<b>DATE</b>
52.204-7	System for Award Management	OCT 2018
52.204-16	Commercial and Government Entity Code Reporting	JUL 2016
52.204-17	Ownership or Control of Offeror	JUL 2016
52.204-18	Commercial and Government Entity Code Maintenance	JUL 2016
52.204-19	Incorporation by Reference of Representations and Certifications	DEC 2014
52.204-21	Basic Safeguarding of Covered Contractor Information Systems	JUN 2016
52.204-23	Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities	JUL 2018
52.209-5	Certification Regarding Responsibility Matters	OCT 2015
52.209-7	Information Regarding Responsibility Matters	OCT 2018
52.216-7	Allowable Cost and Payment. Fill-in: (a)(3): See Section G	AUG 2018
52.222-2	Payment for Overtime Premiums Fill-in: (a): 0	JUL 1990

SECTION I – CONTRACT CLAUSES

<b>FAR</b>	<b>TITLE</b>	<b>DATE</b>
52.224-3	Privacy Training	JAN 2017
52.232-18	Availability of Funds	APR 1984
52.232-22	Limitation of Funds	APR 1984
52.232-23	Assignment of Claims	MAY 2014
52.232-25	Prompt Payment (Alternate I)	FEB 2002
52.233-2	Services of Protest	SEP 2006
52.237-10	Identification of Uncompensated Overtime	MAR 2015
52.242-1	Notice of Intent to Disallow Costs.	APR 1984
52.242-3	Penalties for Unallowable Costs	MAY 2014
52.242-15	Stop-Work Order. Alternate I	APR 1984
52.243-2	Changes—Cost Reimbursement. Alternate I	APR 1984
52.244-2	Subcontracts Fill in: (d) In support of CLINs X001 and X002 (j) TBD	OCT 2010
52.245-1	Government Property	JAN 2017
52.246-3	Inspection of Supplies—Cost-Reimbursement	MAY 2001
52.246-5	Inspection of Services—Cost-Reimbursement	APR 1984
52.246-16	Responsibility for Supplies	APR 1984
52.247-34	F.O.B Destination	NOV 1991
52.249-6	Termination (Cost-Reimbursement)	MAY 2004
52.249-14	Excusable Delays	APR 1984

## SECTION I – CONTRACT CLAUSES

### **I.2.1 FAR CLAUSES INCORPORATED BY FULL TEXT**

#### **FAR 52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (AUG 2020)**

(a) *Definitions.* As used in this clause—

*Backhaul* means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

*Covered foreign country* means The People’s Republic of China.

*Covered telecommunications equipment or services* means—

- (1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);
- (2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);
- (3) Telecommunications or video surveillance services provided by such entities or using such equipment; or
- (4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

*Critical technology* means—

- (1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;
- (2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-
  - (i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or
  - (ii) For reasons relating to regional stability or surreptitious listening;



## SECTION I – CONTRACT CLAUSES

- (3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);
- (4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);
- (5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or
- (6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

*Interconnection arrangements* means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

*Reasonable inquiry* means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

*Roaming* means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

*Substantial or essential component* means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) *Prohibition.* (1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies

## SECTION I – CONTRACT CLAUSES

or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) *Exceptions.* This clause does not prohibit contractors from providing—

- (1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or
- (2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at <https://dibnet.dod.mil>. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at <https://dibnet.dod.mil>.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

- (i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.
- (ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

## SECTION I – CONTRACT CLAUSES

(End of clause)

### **FAR 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)**

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed six months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 calendar days of the end of the PoP.

(End of clause)

### **FAR 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)**

- a. The Government may extend the term of this contract by written notice to the Contractor within **30 days**; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least **60** calendar days before the contract expires. The preliminary notice does not commit the Government to an extension.
- b. If the Government exercises this option, the extended contract shall be considered to include this option clause.
- c. The total duration of this contract, including the exercise of any options under this clause, shall not exceed 66 months.

(End of clause)

### **FAR 52.229-8 — TAXES — FOREIGN COST-REIMBURSEMENT CONTRACTS (MAR 1990)**

- a. Any tax or duty from which the United States Government is exempt by agreement with the Government of any nation within the AOR of USAFRICOM, USCENTCOM, USEUCOM, USNORTHCOM, USPACOM, and USSOUTHCOM, or from which the Contractor or any subcontractor under this contract is exempt under the laws of any nation within the AOR of USAFRICOM, USCENTCOM, USEUCOM, USNORTHCOM, USPACOM, and USSOUTHCOM, shall not constitute an allowable cost under this contract.
- b. If the Contractor or subcontractor under this contract obtains a foreign tax credit that reduces its Federal income tax liability under the United States Internal Revenue Code (Title 26, U.S. Code) because of the payment of any tax or duty that was reimbursed under this contract, the amount of the reduction shall be paid or credited at the time of such offset to the Government of the United States as the Contracting Officer directs.

(End of clause)

## **I.3 GSAM CLAUSES INCORPORATED BY REFERENCE**

The full text of a clause may be accessed electronically at the GSAM website:

TO 47QFCA21F0001  
P00024

Page I-6

## SECTION I – CONTRACT CLAUSES

<https://www.acquisition.gov/gsam/gsam.html/>

GSAM	TITLE	DATE
552.232-39	Unenforceability of Unauthorized Obligations (FAR Deviation)	FEB 2018
552.232-78	Commercial Supplier Agreements Unenforceable Clauses	FEB 2018
552.239-70	Information Technology Security Plan and Security Authorization	JUN 2011

### **I.3.1 GSAM CLAUSES INCORPORATED BY FULL TEXT**

#### **GSAM 552.212-71 CONTRACT TERMS AND CONDITIONS APPLICABLE TO GSA ACQUISITION OF COMMERCIAL ITEMS (JUNE 2016)**

As prescribed in 512.301(a) (1), insert the following clause:

Contract Terms and Conditions Applicable to GSA Acquisition of Commercial Items (Jul 2003)

(a) The Contractor agrees to comply with any clause that is incorporated herein by reference to implement agency policy applicable to acquisition of commercial items or components. The clause in effect based on the applicable regulation cited on the date the solicitation is issued applies unless otherwise stated herein. The clauses in paragraph (b) of this section are incorporated by reference:

(b) Clauses.

552.203-71 Restriction on Advertising

552.211-73 Marking

552.215-70 Examination of Records by GSA

552.229-70 Federal, State, and Local Taxes

552.232-23 Assignment of Claims

552.237-71 Qualifications of Employees

(End of clause)

### **I.4 DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT (DFARS) CLAUSES**

The full text of a clause may be accessed electronically at Defense Procurement and Acquisition Policy website:

[www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html/](http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html/)

## SECTION I – CONTRACT CLAUSES

DFARS	TITLE	DATE
252.216-7005	Award Fee	FEB 2011
252.225-7007	Prohibition on Acquisition of Certain Items from Communist Chinese Military Companies	DEC 2018
252.225-7040	Contractor Personnel Supporting U.S. Armed Forces Deployed Outside the United States	OCT 2015
252.225-7972	Prohibition on the Procurement of Foreign –Made Unmanned Aircraft Systems (DEVIATION 2020-O0015)	MAY 2020
252.225-7973	Prohibition on the Procurement of Foreign-Made Unmanned Aircraft Systems – Representation (DEVIATION 2020-O0015)	MAY 2020
252.227-7000	Non-estoppel	OCT 1966
252.227-7013	Rights in Technical Data - Noncommercial Items Fill in: (e)(3): No assertions	FEB 2014
252.227-7014	Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation Fill in: (e)(3): No assertions	FEB 2014
252.227-7017	Identification and Assertion of Use, Release, or Disclosure Restrictions. Fill-in: (d). No assertions.	JAN 2011
252.227-7028	Technical Data or Computer Software Previously Delivered to the Government	JUN 1995
252.239-7010	Cloud Computing Services	OCT 2016
252.239-7017	Notice of Supply Chain Risk	FEB 2019

### **I.4.1 CLASS DEVIATION—252.223-7999 ENSURING ADEQUATE COVID-19 SAFETY PROTOCOLS FOR FEDERAL CONTRACTORS (DEVIATION 2021-O0009)**

As prescribed in Class Deviation 2021-O0009, Ensuring Adequate COVID-19 Safety Protocols for Federal Contractors, use the following clause:

**ENSURING ADEQUATE COVID-19 SAFETY PROTOCOLS FOR FEDERAL CONTRACTORS (DEVIATION 2021-O0009) (OCT 2021)**

(a) Definition. As used in this clause –

## SECTION I – CONTRACT CLAUSES

United States or its outlying areas means—

- (1) The fifty States;
- (2) The District of Columbia;
- (3) The commonwealths of Puerto Rico and the Northern Mariana Islands;
- (4) The territories of American Samoa, Guam, and the United States Virgin Islands; and
- (5) The minor outlying islands of Baker Island, Howland Island, Jarvis Island, Johnston Atoll, Kingman Reef, Midway Islands, Navassa Island, Palmyra Atoll, and Wake Atoll.

(b) Authority. This clause implements Executive Order 14042, Ensuring Adequate COVID Safety Protocols for Federal Contractors, dated September 9, 2021 (published in the Federal Register on September 14, 2021, 86 FR 50985).

(c) Compliance. The Contractor shall comply with all guidance, including guidance conveyed through Frequently Asked Questions, as amended during the performance of this contract, for contractor or subcontractor workplace locations published by the Safer Federal Workforce Task Force (Task Force Guidance) at:

<https://www.saferfederalworkforce.gov/contractors/>

(d) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (d), in subcontracts at any tier that exceed the simplified acquisition threshold, as defined in Federal Acquisition Regulation 2.101 on the date of subcontract award, and are for services, including construction, performed in whole or in part within the United States or its outlying areas.

## SECTION J – LIST OF ATTACHMENTS

### **J.1 LIST OF ATTACHMENTS**

The following attachments are attached, either in full text or electronically at the end of the TOR.

<b>ATTACHMENT</b>	<b>TITLE</b>
A	COR Appointment Letter
B	Acronym List
C	Incremental Funding Chart (electronically attached .xls)
D	Award Fee Determination Plan (AFDP)
E	Problem Notification Report (PNR) Template
F	Program Management Report (MSR) Template
G	Trip Report Template
H	Deliverable Acceptance-Rejection Report Template
I	Government Furnished Equipment Listing
J	Department of Defense (DD) 254 (electronically attached .pdf)
K	Organizational Conflict of Interest (OCI) Statement
L	Corporate Non-Disclosure Agreement (NDA)
M	Travel Authorization Request (TAR) Template (electronically attached .xls)
N	Request to Initiate Purchase (RIP) Template (electronically attached .xls)
O	Consent to Purchase (CTP) Template (electronically attached .xls)
P	Status of Forces Agreements (SOFA)
Q	Service Level Agreements (SLA)